Records Management Policy

Table of contents

1 Purpose

This policy applies to all Department of Communities and Justice (DCJ) staff who receive and record digital records and/or digitise hard copy records for capture into an approved electronic document records management system. It outlines how responsibility for records management has been assigned and how staff are expected to contribute to and interact with the records program and implement sound recordkeeping practices.

This policy sets the framework for the creation, capture, management and use of records in all formats to support the transition from paper to digital recordkeeping. The policy also endorses the principles of digital continuity for electronic records to ensure that records are complete, available and useable for as long as needed by all potential users, including for purposes beyond the intended original use.

To support agency business and to meet legal and policy requirements, systems that manage information need to operate so that the records they contain:

- are accurate and can be trusted
- enables information to be managed securely as a valued asset, now and into the future
- are complete and unaltered
- allows the sharing of trusted information with government and with the community
- are managed across the full lifecycle, protected from unauthorised use and inappropriate deletion are findable and readable
- can be proven to be genuine.

2 Definitions

Term	Definition
State record	Any record, made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a public office (*State Records Act 1998*, s.3 (1)).
Business systems	Systems that create, process and manage data to support business processes.
Corporate records	All corporate information which is evidence of the business of the DCJ including decision, actions, transactions, communications and outputs.
Custodian	A delegate responsible for the safe use, proper custody, security and maintenance of corporate information and records.

Term	Definition
Disposal	The destruction of records or their transfer to NSW State Archives and Records.
Disposal authority	A disposal instrument approved by the NSW State Archives and Records Authority Board. A disposal authority identifies the records required as state archives and provides approval for the destruction of other records after the mandatory minimum retention periods have been met.
Documents	Structured units of recorded information, published or unpublished, in hard copy or electronic form and managed as discrete units in information systems.
EDRMS	Electronic document and records management system
Electronic records	Any information that is recorded in a form that only a computer can process and that satisfies the definition of a record may include: computer records, video, audio data. Records may be born digital, or converted to electronic format as a result of scanning or digitisations.
Employees	All personnel employed by the Department of Communities and Justice. This includes all permanent and non-ongoing staff, consultants and contractors.
Files/containers	A file is a collection of documents that show organisational activities through an identifiable sequence of transactions.
Inactive records	Records no longer required for use by the organisation in the conduct of its activities and functions.
Information management	The discipline and organisational function of managing records to meet operational business needs, accountability requirements and community expectations.
Information management systems	Specific applications used to maintain, manage and provide access to an organisations record resources.
Information security	The preservation of the confidentiality, integrity and availability of information.
Metadata	Data describing data and data systems. Information that is used to facilitate intellectual control of, and structured access to, other information. For example, when data was captured, who has accessed it, if/when/how it has been edited or altered.
Personal information	Correspondence that is of a private or non-public nature, that relates solely to an individual's own affairs that do not relate to or have any effect upon the conduct of DCJ business.

Term	Definition
Records	Records are the information, regardless of format or media, created, received, or maintained by employees in the course of DCJ business which are evidence of business activities and transactions as well as the associated actions, decisions, outputs, and outcomes.
Recordkeeping	Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.
Records management program	A records management program encompasses the management framework, the people and the systems required within DCJ to manage full and accurate records over time. This includes the identification and protection of records with longer-term value that may be required as state archives.
Sentencing	Applying a disposal authority to a record.
State record	Any record made and kept or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office or for the use of a public office. (*State Records Act 1998*, s.3 (1)).

3 Scope

This policy covers all divisions of DCJ. It applies to all officers, consultants, contractors, and service providers who have been contracted to undertake outsourced DCJ business activities.

This policy applies to all hard copy and digital records created and captured in the course of the normal business activities of DCJ, including:

- records and information managed in all business processes
- information in all business systems
- records held in all formats including audio and visual.

This policy applies to all records and associated metadata from the time of creation or capture and covers:

- all DCJ staff, regardless of employment type
- all aspects of DCJ's business operations
- all types and formats of records created to support business activities
- all business applications used to create records

- organisations and businesses, including their employees, to which DCJ has outsourced its functions or activities, and therefore associated recordkeeping responsibilities.

All staff are accountable for the efficient, effective and appropriate use, management and security of records and information resources that are received, created, acquired or retained in the performance of official duties.

All staff are to record and update the location of each record with every movement of the record. This ensures that records, as assets, can be accounted for in the same way that other assets of DCJ are.

4 Policy statement

DCJ's records are its corporate memory and a vital asset for ongoing accountability. Good recordkeeping is critical to corporate governance and operational efficiency, provides essential evidence of business activities and transactions, and demonstrates accountability and transparency in the decision-making processes.

DCJ is committed to implementing and maintaining best practice recordkeeping policy, practice and procedure and to support agency business, and meet legal and policy requirements. Systems that manage information need to operate so that records can be proven to be genuine: are accurate and can be trusted, are complete and unaltered, are secure from unauthorised access, alteration and deletion, are findable and readable and are related to other relevant records.

This policy outlines the principles for effective records management for DCJ. It complements the Information Management Policy and creates the framework for managing records in all formats that are created, received and used in the conduct of DCJ business.

DCJ is transitioning to digital recordkeeping in line with NSW Government policies to conduct business digitally, as far as is practical. This policy supports the changing administrative structure, functions and technology environment of DCJ. In this respect, a key aspect of DCJ approach to records management is to determine electronic business systems that need to be managed as records management systems. Before a decision is made to acquire, develop or upgrade an electronic business system, the records management capability of the system must be considered.

The key objectives of this policy seek to ensure that:

- records of all activities and decisions are created, managed and retained for the length of time required
- records are managed efficiently and effectively in support of business objectives
- records are stored appropriately and as cost-effectively as possible

- when no longer required records are disposed of in a timely and efficient manner in accordance with the records policy and using the appropriate disposal authority
- digital and other technology dependent records are maintained in an authentic and accessible form for as long as they are required in accordance with this policy
- records can be easily accessed and used for as long as they are required.

5 Related legislation and documents

DCJ is accountable to Ministers, NSW Parliament, clients and the public for its decisions and actions and operates within a highly regulated environment.

To achieve good management practice, DCJ is responsible for maintaining records that document its administration having regards to legislation requirements, regulations and standards.

To meet and support its obligations, DCJ has regard to records management legislation and standards for recordkeeping, as well as access and security and privacy protection which apply to all NSW Government agencies.

5.1 Legislation

Good government recordkeeping, and its effective management, are essential to sound management of government business, to the delivery of quality services to the people of NSW and to public accountability. The government expects high standards in recordkeeping across government as it does in respect of any other aspect of public management. Staff must be aware of the legislation, regulations and standards that govern how records should be managed, in order to comply with NSW laws.

Key records management provisions of the *State Records Act 1998* require public offices to:

- make and keep records that fully and accurately document their operations and administration
- establish and maintain a records management program in conformity with standards and codes of best practice approved by NSW State Archives and Records
- ensure that records are stored in conditions appropriate to their format and preservation requirements
- ensure that records held in digital or other technology dependent formats are accessible for as long as they required
- ensure records are managed in accordance with the *Privacy and Personal Information Protection Act 1998* (PPIP Act), the *Government Information (Public*

Access) Act 2009 (GIPA Act) and the *State Records Act 1998*. These obligations are set out in the department's privacy policy and management plan.

5.2 Standards

Recordkeeping standards are mandatory, measurable and include minimum compliance requirements. They are outcomes oriented, rather than prescriptive.

Standards issued by NSW State Archives and Records under the Act include:

- Standard on the physical storage of state records: The purpose of this standard is to establish minimum requirements for the storage of physical state records and to guide decisions for storing records.
- Standard on records management: This standard establishes the requirements for effective records and information management.

The Principal Manager Records is to be informed as soon as practicable of any actual or suspected breach of this policy. Non-compliance or breaches of this policy, without an appropriate exception could leave DCJ open to criticism in an investigation where recordkeeping practices were an issue. This would be investigated and misconduct escalated with Human Resources. Failure to comply with a code of best practice may result in disciplinary action in accordance with the department's code of conduct.

Compliance to the above standards supports compliance with the *State Records Act 1998*.

5.3 Regulations

Whole-of-government policies and directives issued by the Department of Premier and Cabinet, Treasury, the Public Service Commission or the Department of Customer Service can also establish requirements with respect to the making, keeping and management of records.

Cyber Security NSW have carriage of Cyber Security Policy and the requirement to report to SARA on any "cyber incident that involves information damage or loss" *https://www.digital.nsw.gov.au/policy/cyber-security-policy/roles-and-responsibilities*

6 Roles and responsibilities

DCJ is part of the Stronger Communities cluster. All business records created in DCJ belong to DCJ and are State records. Management and control of these records is the responsibility of every person in DCJ. The other departments within the Stronger Communities cluster are responsible for the management and control of their own records. This management extends to records and information in all formats, in all business environments and in all types of systems.

DCJ may obtain support for recordkeeping and records management from an internal shared service provider or an external provider. However the responsibility for appropriate management and control remains with DCJ.

In the event of an administrative/machinery of government change that impacts the location of functions across government, the responsibility for the management and control of records follows that transfer of functions. Guidelines have been issued by NSW State Archives and Records for the accountable transfer of records in this instance.

Compliance with this policy by all staff, including consultants, contractors, and service providers who have been contracted to undertake outsourced DCJ business activities is mandatory. All officers working for DCJ have a responsibility to follow this policy and to maintain sound recordkeeping practices in their daily work. This policy supersedes all previous recordkeeping and records management policies.

The main roles and responsibilities for implementation of this policy are as follows:

6.1 The Secretary

The Secretary of DCJ is responsible for:

- compliance by DCJ cluster with the requirements of the *State Records Act 1998* and the standards and requirements issued under the Act (Section 10 of the Act)
- allocating responsibility for records and information management throughout the organisation down through various levels of management
- holding ultimate responsibility for records and information management in accordance with business requirements and relevant legislation.

6.2 Chief Information Digital Officer and Chief Information Technology Officer

The Chief Information Digital Officer and Chief Information Technology Officer are responsible for:

- providing IT infrastructure and resources to ensure successful operation of records management systems
- resourcing and supporting the technical implementation of the records management system.

6.3 Director, Information Management

The Director of Information Management is responsible for:

- providing strategic direction and oversight of the records management program
- issuing the DCJ Records Management Policy and DCJ corporate records and information strategies

- issuing standards and procedures consistent with this policy
- reporting to the Executive on the Records Management Program
- ensuring the records management program meets business needs and complies with relevant legislation and regulations
- ensuring DCJ has skilled records management staff or access to appropriate skills
- identifying systems and repositories containing records and their business owners
- building capability in DCJ for managing high risk records and systems.

6.4 Principal Manager Records

The Principal Manager Records is identified as the Senior Responsible Officer for records management for DCJ. The Principal Manager Records liaises with Senior Responsible Officers for records management at the Crown Solicitor's Office, NSW Fire and Rescue and any other entities within the DCJ cluster.

The Principal Manager Records is responsible for:

- cooperating and liaising with NSW State Archives and Records
- providing records management policies, procedures and business rules which support business and comply with legal and regulatory requirements
- identifying and mitigating risks to records and information
- responding to monitoring/reporting requests from the State Archives and Records Authority of NSW.
- reporting any cyber incident that involves information damage or loss of records to NSW State Archives and Records (as per requirement in *https://www.digital.nsw.gov.au/policy/cyber-security-policy/roles-and-responsibilities*)
- identifying systems and repositories containing records and their business owners
- developing key performance indicators around elements of the records management program, including capture, storage, maintenance and monitoring, disposal and transfer of records
- monitoring and reviewing performance and compliance of the records management program to assess how it meets business needs and accountability requirements
- identifying all records and information required to meet or support business and recordkeeping requirements, including accountability and community expectations

- design and oversight of records disposal processes and documentation, including the approval of records destruction, identification of state archives and transfer of custody and/or ownership of records and state archives
- working with business managers to confirm that management strategies are in place to ensure that high risk, high value areas of business and systems managing such business are identified and assessed, and that records and information management is integrated into high risk and high value business activities, systems and processes
- to identify and address records management requirements in contractual arrangements for outsourced, cloud or other service providers based on risk assessments
- to identify and advise business unit managers on the requirements for recordkeeping in outsourcing and service delivery contracts
- ensure that access to records and information is managed appropriately in accordance with legal and business requirements.

It is the responsibility of the Principal Manager Records to monitor and update this policy when required. This policy will be reviewed annually and earlier when any significant new information, legislative or organisational change warrants amendments.

6.5 Records Management Unit

Staff in the Records Management Unit are responsible for:

- providing advice and guidance to support the maintenance and protection of records when technology, systems, services and processes change
- provide online training, guidelines and advice
- regularly updating training material and the records management home page on the DCJ intranet
- liaising with NSW State Archives and Records regarding approval and maintenance of retention and disposal authorities
- providing advice regarding records disposal processes and documentation, including the destruction of records, identification of state archives and transfer of records to the Government Records Repository (GRR)
- providing records management control tools to govern how records are created, captured and stored, including developing business rules and procedures in collaboration with business managers
- providing advice to DCJ employees regarding the creation and maintenance of DCJ records and the systems in which they are maintained and;

- providing access to records in secondary storage and designated as state archives, in accordance with access directions, where records are not open to public access by default.

6.6 All managers

All managers are responsible for:

- incorporating records management responsibilities into staff role descriptions and performance management plans
- ensuring staff understand their obligation to comply with the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002* when handling personal information
- ensuring records management is integrated into business activities, systems and processes
- ensuring staff have the knowledge of systems and local business rules to capture records of work they do and use to do their work
- working with the Records Management Unit staff to improve records and information capabilities
- ensuring staff including consultants, contractors, and service providers who have been contracted to undertake outsourced DCJ business activities comply with this policy
- monitoring staff to ensure they understand and comply with the Records Management Policy and associated procedures
- advising the Principal Manager Records of high risk and high value areas of business and the information captured, used and managed in such business
- planning and managing business activities involving the collection of information and the creation of records in accordance with business needs and regulatory requirements, including protecting sensitive records
- ensuring staff engage in records management and privacy training and professional development opportunities.

6.7 Project Sponsor/Leads

Project Sponsor/Leads are responsible for:

- supporting the owner and custodian in the identification and prioritisation of records management improvement initiatives
- determining that all legal, regulatory and policy requirements are met in relation to the management of the records.
- controlling any risks associated with the project

- ensuring records and information requirements are considered and that records are maintained and protected when technology, systems, services and processes change
- advising the Principal Manager Records that records and information management risk have been considered as part of the development process when moving to a new service environment, systems or service (including cloud based services), or when improving existing work processes, systems or services
- ensuring that records management requirements are incorporated in contractual arrangements for outsourced, cloud or other service providers based on risk assessments.

6.8 Non-government organisations, contractors and consultants

Non-government organisations (NGOs), contractors and consultants undertaking work for DCJ are subject to the same guidelines as DCJ staff and must be familiar with and comply with the DCJ policy and guidelines on the management of information and records.

They have responsibility for:

- understanding their obligations to comply with *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*
- understanding their responsibility for creating and capturing accurate records of their actions, decisions and events, to provide evidence of their decisions/work, including making records of work where records are not automatically created (e.g. minutes of meetings, notes of telephone conversations)
- ensuring the return of all records created or used as part of the service arrangement when required as all records created and managed during the service arrangement remain the property of DCJ
- ensuring that those records that have personally been created are used solely for the purposes for which they were created, unless otherwise lawfully authorised, for example postal addresses, telephone numbers and email addresses
- notifying the relevant DCJ business units of any inadvertent disclosure or loss of information held by NGOs, contractors and consultants.

6.9 All staff

All employees are accountable for the efficient, effective and appropriate use, management and security of records and information resources that are received, created, acquired or retained in the performance of official duties.

They also have responsibility to:

- understand the records management responsibilities associated with their role and the need to keep records

- understand their obligations to comply with the obligations set out in the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*
- understand their responsibility for creating and capturing accurate records of their actions, decisions and events, to provide evidence of their work, including making records of work where records are not automatically created (e.g. minutes of meetings, notes of telephone conversations)
- know and apply the Records Management Policy and associated procedures
- use records management control tools to create, capture and maintain full and accurate records of business activities as business is conducted
- use and share records appropriately to support collaboration and authorised re-use of information. For example, DCJ may be unwilling to share a dataset publicly because of the risk of identifying individuals. However, DCJ may be comfortable with sharing that dataset with data protections in place, such as the removal of names and addresses, and as long as it is only accessed by authorised staff
- undertake records management and privacy training and professional development
- understand the requirements for retaining and disposing of records
- know and apply requirements for creating, capturing and managing personal records
- protect records from inappropriate or unlawful access, loss or damage
- ensure that those records that have personally been created are used solely for the purposes for which they were created, unless otherwise lawfully authorised
- notifying their manager and ensuring that any loss of a record, hardcopy, on USB etc is communicated to the Director, Open Government, Information and Privacy, Law Reform and Legal Services.

7 Authorised recordkeeping systems

DCJ records must be captured and maintained on official DCJ infrastructure.

Content manager (formerly known as TRIM) is the primary electronic document and record management system for DCJ. It manages both physical and electronic records (documents and files/containers) along with the required associated metadata.

DCJ also uses client information systems (CIS) which is a comprehensive, integrated system of clinical, administrative, and financial records that provides information necessary and useful to deliver client services. Information may be maintained electronically, in hard copy or both.

OneSAP is also an authorised recordkeeping system. SAP stands for Systems Applications and Products in Data Processing and is the name of the platform used by DCJ for human resources and financial recordkeeping and transactions.

DCJ records (irrespective of format) stored in shared drives, personal drives, email folders, SharePoint sites, workstations and on backup disks or drives e.g. USB drives are not compliant with DCJ's recordkeeping obligations. These drives and locations are not compliant because they:

- do not capture sufficient metadata to meet the legal recordkeeping requirements for retention and disposal
- do not allow records to be widely searchable or accessible to all who need them
- are not authenticated and are not secure from alteration or deletion.

This business information remains non-compliant until it is registered as a record in Content Manager or an authorised business system.

A business information system (BIS) is an information reporting and/or transaction system used within DCJ. Business information systems are not automatically records management compliant – they contain structured data that potentially constitutes part of a record but this does not by default contain the contextual information to ensure reliability, authenticity and usability. Further, legal recordkeeping retention and disposal requirements (beyond keeping backups of data) are usually not adequately catered for.

Before being authorised to store and manage records, all DCJ business information systems must be assessed by the Principal Manager Records in consultation with relevant stakeholders. All BIS must be able to collect all information required for the activity – it should be fit for purpose and:

- capture content, structure and context of the record
- provide adequate and compliant storage of records
- provide protection of record integrity and authenticity
- ensure the security of records
- be readily accessible to all staff who need to use the records contained within the system, for as long as the record is needed
- undertake the disposal of records in accordance with approved disposal authorities
- ensure the recoverability of records in the event of a disaster
- ensure the availability of records in a useable format through technology changes and migration.

DCJ staff are encouraged to utilise a business system checklist that has been developed by NSW State Archives and Records to assess whether their business

system is compliant as a recordkeeping system. Undertaking an assessment upfront helps define technical specifications needed to ensure that the organisation's recordkeeping requirements are addressed and considered.

The checklist offers a basic recordkeeping functionality assessment. When planning to procure or implement new systems, or when prioritising further developments of existing business systems consideration organisations should be given to:

- the value of the records that are or will be created in and/or managed by the business system and category of records, e.g. Cabinet
- the risks associated with the business that the system supports
- inherent information risks
- any recordkeeping requirements that relate specifically to the business being conducted
- the organisational context in which the business system operates (when making decisions about any remedial work that may be required)
- whether the business the system supports is subject to any recordkeeping requirements
- how well the system is currently functioning as a recordkeeping system
- what action may be required to enable the system to meet recordkeeping requirements.

Please refer to the NSW State Archives and Records website for the most current version of the checklist.

8 Records retention and disposal authorities

Under the *State Records Act 1998*, State records may only be disposed of with the authority of the NSW State Archives and Records, or via normal administrative practice as defined in section 22 of the Act.

Records and information are kept for as long as they are needed for business, legal and accountability requirements. Records and information are sentenced according to current authorised retention and disposal authorities.

Please refer to the NSW State Archives and Records website for the most current version.

Further advice and support regarding records disposal authorities and how to implement them is available by lodging a request to Records Management Unit through ServiceNow.

9 Definition of a record

Records are evidence of business conducted by an organisation. Any reference to a record in this policy refers to records in any format as defined in the *State Records Act 1998*.

DCJ staff are responsible for keeping a record of business activities conducted as part of their role.

Examples of business activities include:

- actions
- decisions
- events
- conversations
- advice
- contracts and agreements
- client interaction or activities
- directions (operational, financial and other)
- inputs and outputs
- statistics and reporting
- formation of policy and procedure
- maintenance of inventories and registers maps or plans.

Records can be held in any format. This includes but is not limited to:

- data in business systems – e.g., SAP, ChildStory, CIMS, OIMS
- hard copy information including work diaries (printed, handwritten)
- electronic (born digital) documents – e.g. Word, Excel, Power Point
- electronic files – e.g. EDRMS containers
- electronic messaging – e.g. email, voicemail, instant messaging SMS (short message service), multimedia message service (MMS).Please note that staff should not be using personal messaging services such as email for business related work
- corporate social media – e.g. Twitter, Facebook, LinkedIn, blogs, wikis, discussion boards/forums
- web content – e.g. agency approved intranet and internet sites
- photographs – e.g. official photographs documenting business activities

- videos – e.g. agency approved YouTube, Vimeo, webinars, video conferencing, teleconferencing, video instant messaging and podcasts
- models, plans and architectural drawings
- survey tools.

SharePoint and social media are forms of collaboration and communication which allow users to collaborate on the creation, review and approval of various types of content, including documents for the department, however they are not recordkeeping systems (i.e. a system purposely designed to capture, maintain and provide access to records over time). For SharePoint to be used as a compliant recordkeeping system, it must be configured and/or enhanced with add-on software to enable staff to capture, identify and classify records so that their content, structure and context of creation are fixed in time and space. This facilitates the making of complete, authentic and usable records.

Staff who use these tools for their work should be aware that content published in this media may constitute as a record as defined in this policy. DCJ records should only be on agency approved systems. Personal email messaging and personal social media sites should not be used to create or store DCJ records. Guidance regarding the capture of records and associated metadata, from communications conducted via social media platforms, are provided on the intranet and are to be followed.

DCJ information stored physically or on electronic and computing devices whether owned or leased by DCJ, the employee or a third party, remains the sole property of DCJ. Use of instant messaging or MMS for key business decisions must be transferred to a compliant records management system.

Social media information is a record under the definitions of the *State Records Act 1998*. This does not mean that all social media information must be captured and managed as an official record but it does mean that some high risk and key business value social media information will need to be managed and kept for appropriate periods of time.

For a record in digital format to be meaningful and to serve as admissible evidence of a business transaction, it must have full and accurate metadata to provide adequate context and to support its authenticity and management over time. This will help to ensure that DCJ's business, accountability and archival requirements are met in a systematic and consistent way, and that digital records are described, reliable, meaningful, admissible as evidence, accessible, sharable and re-usable for as long as they lawfully need to be retained.

9.1 Outsourcing

DCJ conducts its business using both internal resources and outsourcing arrangements. This policy applies to any party contracted to perform services to/for DCJ.

Outsourcing can take many forms, including:

- engaging a private sector organisation, contractor or consultant
- funding agreements with not-for-profit or non-government organisations/funded service providers
- sharing arrangements with other government agencies e.g. a small office using the resources of a larger office
- shared services internal to DCJ and cluster agencies
- shared services procured from centralised whole-of-government services, or from private sector organisations.

The *State Records Act 1998* does not apply to private sector service providers as a matter of course. DCJ records management requirements must be incorporated into all procurement, contractual or other government arrangements for outsourcing, cloud or other service providers. Each contract/arrangement should specify how those requirements will be monitored and reported for compliance. Guidance on appropriate wording of these obligations in contractual arrangements can be obtained from Law Reform and Legal Services, DCJ.

Where DCJ makes outsourcing arrangements with other government agencies the *State Records Act 1998* will apply and it remains appropriate to specify records management requirements in these contractual agreements or service level agreements.

10 Document information

Document name	Records Management Policy
Applies to	All of DCJ
Replaces	FACS Records Management Policy Justice Records Management Policy VS Records Management Policy Electronic Records Management Policy
Document reference	D20/646903
Approval	ICT sub - committee 6 August 2020
Version	1.0
Commenced	24 August 2020
Due for review	24 August 2022
Policy owner	Director, Information Management

11 Support and advice

For support, advice or further information contact:

Business unit	Information and Digital Services Corporate Services
Email	RecordsManagementFACS@facs.nsw.gov.au