Commissions of Inquiry Records and Information Handbook

DJAG ICT HANDBOOK				
Version	**Status**	**Approver**	**Effective date**	**Next review**
1.0	Approved	DJAG Chief Information Officer	09/02/2023	09/02/2025
			Security classification	OFFICIAL

Contents

1 Introduction

1.1 Purpose

This Handbook serves two purposes: firstly, to help Commissions of Inquiry manage their records and information while they are in progress; and secondly, to enable them to meet the quality expectations of the Department of Justice and Attorney-General (DJAG) for the transfer of records and information after they finish.

1.2 Audience

This Handbook is targeted specifically at Commission of Inquiry (COI) staff with records and information management responsibilities, such as the Executive Director, Business Manager, Administrative Assistants, System Administrators and other roles.

2 Background

2.1 Records management

COIs are required to comply with the *Public Records Act 2002*. This means Commission staff must create and maintain records that document their business activities. Those records must also be managed appropriately while the Commission exists and after it finishes.

2.2 Information security

COIs should work with their administering agency to identify and manage information security risks. A key part of this is classifying sets of information (including records) based on their business impact and implementing appropriate controls to manage the identified risks.

The Queensland Government Information Security Classification Framework (QGISCF). outlines the responsibilities for entities to security classify information and is a minimum requirement of the Queensland Government Information Security Policy (IS 18).

2.3 Default responsible public authority

After COIs finish, their records will normally become the responsibility of the Department of Justice and Attorney-General (DJAG). DJAG will take custody of and manage those records until they are transferred to Queensland State Archives (QSA) or destroyed under the relevant retention and disposal schedule.

In exceptional circumstances, another agency may become the responsible public authority for COI records.

3 Guidance

3.1 Managing records

COI staff with records management responsibilities should carry out the following actions:

- Roles. Confirm and document which roles have overall operational responsibility for the Commission's records (for example, the Business Manager).
- Guidance. Develop records management guidance which sets out how to manage records across the different ICT applications that Commission staff may be using, such as shared network drives, Microsoft 365 (Outlook, SharePoint, OneDrive, etc), case management systems, electronic document and records management systems (eDRMS) and any others.

This guidance should describe how each application is to be used and where the formal records of the Commission should be saved. It should also emphasise the importance of creating and managing records in digital format wherever possible.

- Filing structures. Establish appropriate filing structures for the Commission's digital records. These are key to making records easy to find and access and will save time when preparing records for handover to DJAG. COI filing structures will depend on the type of ICT applications being used, but eDRMS filing structures are recommended to follow a standard Function/Activity/Subject model. A template example of this kind of filing structure is available at the end of this document. It can be tailored to take account of the Commission's unique processes and subject-matter. Establishing practical document naming conventions will also help staff to organise and find records.
- Sentencing. The term sentencing refers to the records management process of matching your information to the relevant retention and disposal schedule to establish the value of the information and the minimum period it must be kept. Records should be sentenced at the file or folder level. There is no need to sentence documents individually. This data can be captured in a control spreadsheet if the ICT application holding the records does not have any built-in retention and disposal functionality. While the COI is in progress, two disposal schedules apply that direct how long you must keep your records:
  1. Commissions of Inquiry Retention and Disposal Schedule.

     This schedule is for COI-specific records including activities relating to establishing, operating and administering the Commission, including managing its terms of reference, appointing members, legal status, investigations and reporting. This information is largely required to be permanently retained by the State as a historical record.
  2. General Retention and Disposal Schedule (GRDS).

     This schedule is for routine administrative matters such as HR and financial processing. These records have a temporary value and will be kept as long as the retention period specifies and then will be destroyed.

     Records with very short-term value only may be disposed of under the GRDS once their business use has ceased. See the 'Transitory and Short Term' records classes at the end of the Schedule. Examples include: invitations, event confirmations and registrations, attendance and guest lists, parking arrangements, bookings, running sheets and checklists, equipment and property booking forms, and clean print outs of digital records.
- Liaise with DJAG. Contact the Information Management Team from the Department of Justice and Attorney-General (DJAG IM Team) as soon as possible after the Commission is established. This will help to achieve a smooth and timely handover of records to DJAG after the Commission ceases.
- Confirm responsible public authority. Arrange for a letter to be sent from the Commission to the Director-General of DJAG, proposing that DJAG become the responsible public authority for the Commission's records after it ceases.
- Once DJAG has accepted responsibility for the records, arrange for a letter to be sent from the Commission to QSA confirming this.
- Digital signatures. Decide if the Commission will use digital signatures in its day-to-day work. Before making a decision, check you can meet relevant legislative requirements and be aware of the risks surrounding different kinds of signatures.
- Document processes for using digital signatures in higher-risk settings, for example, when signing legal documents or using them on behalf of other staff. Ensure that they are securely stored.

- Avoid using images or pictures of hard-copy signatures where possible. These are more difficult to control and authenticate than other kinds of digital signatures, and so increase the risk of inappropriate use and fraud.
- Further general advice on digital signatures can be found on the Queensland Government Enterprise Architecture website and the Crown Law website.
- Working with external providers. Develop requirements for external records and information management providers, for example, eHearing vendors. These requirements should include expectations relating to quality, timeliness, accessibility, security, the retention, return and disposal of records, and so on.
- Scanning records. Hard-copy records may be scanned to make them more accessible. Set up and maintain some basic quality assurance procedures if the Commission is going to scan a significant number of records. Check that the scans are accurate, complete and fit-for-purpose, and ensure they have captured non-standard items such as handwritten notes, colours, diagrams and pictures.

  The preferred file format for scanned documents is text searchable .PDF/A. If the COI's scanning devices cannot generate .PDF/A format scans, .PDF is an acceptable alternative.

  It is usually unnecessary to develop detailed technical requirements relating to resolution, bit-depth and file compression when scanning documents to increase the accessibility of the hard-copy originals rather than to replace them.
- Retaining hard-copy records after scanning. Note that hard-copy records cannot be destroyed after scanning. The originals must be kept and managed. Ensure that Commission staff are aware of this requirement.

Further guidance on managing COI records can be found on the QSA website.

3.2 Managing information security

COI staff with records and information management responsibilities should carry out the following actions:

- Information security classifications. Security classify COI information in line with the Queensland Government Information Security Classification Framework (QGISCF). The QGISCF outlines the responsibilities for entities to classify information and is a minimum requirement of the Queensland Government Information Security Policy (IS 18).
- Working through the security classification process helps you to understand how sensitive your information is. This will make it easier to manage any resulting information security risks and understand the obligations for applying security controls.
- The possible information security classifications are, from lowest to highest, OFFICIAL, SENSITIVE or PROTECTED and there is specific guidance in managing information in each classification level. The highest classification level used in Queensland is PROTECTED.
- PROTECTED information. Commissions of Inquiry often or usually handle PROTECTED information, for example, submissions from individuals that contain highly sensitive personal details. It is important to identify PROTECTED information at an early stage in the Inquiry and put appropriate controls in place to manage it. Note that some ICT applications may not be sufficiently secure to hold PROTECTED information.
- Procedures. When classifying COI information, follow the administering agency's procedures if possible, but a Queensland government assessment tool is available to use if necessary (registration required). The DJAG IM Team can assist you in accessing the tool.
- Ensure that the classifications are signed off at the appropriate level, for example, by the Commissioner or Executive Director.

- Access permissions. Use the results of the information security classification assessments to confirm access permissions for different categories of records. SENSITIVE or PROTECTED records may need to be locked down to senior Commission staff only.
- Communicate. Inform Commission staff of the approved information security classifications and include them in the records management guidance material.

3.3 Preparing records for handover to DJAG

COI staff with records management responsibilities should complete the following actions before the Commission ceases to ensure the smooth handover of records to DJAG:

- Restricted Access Period notice. The responsible officer will need to complete and organise for the Commissioner to sign a Restricted Access Period (RAP) notice for all Commission records that are covered by the Commissions of Inquiry Retention and Disposal Schedule. Guidance on completing a RAP notice is available on the QSA website.
- Records access requests received after the Commission ceases will be managed in accordance with the RAP notice.
- Filing. Save any unfiled records (for example, individual emails that are records) in the ICT application holding the formal records of the Commission.
- Submissions. Ensure that any submissions falling outside the terms of reference of the Inquiry have been returned to the submitter or destroyed. These actions should be documented. Submissions that fall within the COI's terms of reference but are deemed not relevant to the Inquiry, must be retained for ten years before they can be destroyed.
- Sentencing. Ensure that all records have been sentenced against the Commissions of Inquiry Retention and Disposal Schedule or General Retention and Disposal Schedule. Folders or files that contain records with different retention periods and disposal actions may need to be broken up or restructured.
- Security classifications. Ensure that information security classifications have been completed and signed-off by the Commissioner or Executive Director.
- Copies and print-outs. Destroy any duplicate copies of records and clean print-outs of digital records saved into the COI's formal recordkeeping system. Examples may include print-outs or copies of submissions and exhibits used during hearings. This destruction does not need to be documented.
- Hard-copy records. Box-up any hard-copy records that need to be retained after the Commission finishes. Permanent-value records must be housed in Type 1 archive boxes for later transfer to QSA. These can be ordered from stationery suppliers. The QSA website has further guidance on preparing permanent-value records for transfer.
- Records going to QSA. Records identified for transfer to QSA need to be listed in the Transfer List template. The DJAG IM Team will provide guidance on compiling this.
- Digital records. Identify a contact from the administering agency (for example, a System Administrator) who will be able to arrange the export of digital records and their metadata at the conclusion of the Inquiry, and pass on their details to the DJAG IM Team. The DJAG IM Team will typically ask for a sample export to confirm compliance with record keeping requirements.
- Website. Confirm arrangements for the publication of the final report after approval and ensure that it is kept confidential until released.
- Contact the DJAG IM Team to initiate the transition of the COI website to the DJAG environment. It will take at least three weeks to complete the transition. Work with the COI's

technical support staff to export the website in a format that can be easily transitioned across. HTML is preferred.

- If the website contains dynamic content that will need to be maintained after the transition, inform the DJAG IM Team so that further technical information can be gathered. Domain name ownership for the website will also need to be changed to DJAG.
- Confirm governance arrangements for the Commission website after its transition to DJAG. This may include removing certain documents at a future date or keeping the website available for longer than the standard 10 years.

Note that the DJAG IM Team will check to make sure that these actions have been completed before taking custody of COI records. A checklist is available at the end of this document to help keep track of progress.

3.4 Handing records over to DJAG

To complete the handover of COI records to DJAG, COI staff need to provide:

- RAP notice. Email the signed RAP notice to the DJAG IM Team and place the original with the boxed hard-copy records. This will help DJAG and/or QSA to manage access to the records appropriately after handover.
- Security classifications. Provide the approved information security classifications to the DJAG IM Team. This will help DJAG to manage the records appropriately after handover.
- Hard drive. Provide an external hard drive or thumb drive for the export of digital records. Make sure the drive is encrypted and arrange for the export of all digital records onto it, along with a linked .CSV file holding their metadata. The DJAG IM Team can provide an example of this if required. Double-check that the records are in a useable format and their metadata (including title, creator, dates, information security classification, etc) is accessible and complete.
- Delivery – digital and hard-copy. Arrange a date and time to deliver the digital and hard-copy records to the DJAG IM Team. Email the hard drive or thumb drive password to the DJAG IM Team separately.
- Website. Update the contact details on the website to refer to DJAG. Include a notice on the front page such as:

  'The XXX Commission of Inquiry has now concluded. For any enquiries, please contact the Department of Justice and Attorney-General.'

4 Templates and other resources

- Commissions of Inquiry Retention and Disposal Schedule
- Crown Law Guidance on Digital Signatures
- General Retention and Disposal Schedule
- Information Security Classification Tool
- QSA Preparing and Boxing Records Guidance
- QSA Restricted Access Guidance
- QSA Restricted Access Period Notice Template
- QSA Transfer List Template
- Queensland Government Guidance on Digital Signatures
- Queensland Government Information Security Background

- Queensland Government Information Security Classification Framework (QGISCF)
- Queensland Government Information Security Policy (IS18).

5 COI Records Handover Checklist

Action	Completed
Confirm responsible public authority	
Complete Restricted Access Period Notice	
Save unfiled records	
Process submissions outside COI Terms of Reference	
Sentence records against the COI Retention and Disposal Schedule or General Retention and Disposal Schedule	
Complete information security classifications	
Destroy copies and clean print-outs	
Box-up hard-copy records that need to be retained	
List records going to QSA	
Identify a contact for exporting digital records and inform the DJAG IM Team	
Confirm website arrangements	

6 Example COI eDRMS Filing Structure

xxx COMMISSION OF INQUIRY

ADMINISTRATION

FINANCIAL MANAGEMENT

- Asset registration
- Budgeting
- Purchasing

HUMAN RESOURCE MANAGEMENT

- Arrangements
- Establishment
- Recruitment
- Vacancies

INFORMATION & COMMUNICATION TECHNOLOGY (ICT)

- Application Management
- Security
- Telephones

INFORMATION & KNOWLEDGE MANAGEMENT

- Records

PREMISES MANAGEMENT

- Office accommodation

GOVERNANCE

ADMINISTRATIVE ARRANGEMENTS

- Orders in Council
- Commissioner's Directions (records include rulings, orders or practice directions issued by the Commissioner)
- Counsel Assisting

APPOINTMENTS

- Commissioner
- Counsel Assisting
- Experts / Consultants

MEDIA RELATIONS

- Media Releases
- Media Logs

PLANNING

- Arrangements
- Schedules
- The Commissioner's Diaries and Notebooks

INQUIRY INVESTIGATIONS

HEARINGS

- Week No - <Date Range> (Location) / by name of witnesses

LEAVE TO APPEAR

REGISTERS

- Register (Submissions)
- Register (Exhibits)
- Register (Returns)

SUBMISSIONS

- Submissions provided
- Formal statements
- Summaries

SUMMONS

- Requirement to provide information
- Requirement to provide a written statement
- Summons to attend and give evidence
- Requirement to produce documents

OPERATIONS

ADVICE

- Legal Advice
- Advice provided by expert reference groups
- Advice provided by consultants

CONSULTATION

- Individuals
- Non-Government Organisations
- Government agencies

RESEARCH

- Topic
- Working Documents

REPORT WRITING

DRAFT REPORT
FINAL REPORT
PUBLICATION
RECOMMENDATION DEVELOPMENT