Management of public records

In this advisory:

Introduction

Openness and transparency in government and public authorities are in the public interest, and key to promoting integrity and accountability in the public sector. One critical aspect is diligence in creating, maintaining and disposing of public records.

Under the *Public Records Act 2002* staff of public authorities are obliged to manage public records responsibly, and the disposal of public records without authorisation from the State Archivist is a criminal offence.

Public authorities: For the purpose of administering public records, the term 'public authority' covers all state and local government entities including state government ministers, ministerial staff, parliamentary secretaries and public sector agencies including state government departments, government-owned corporations, statutory entities, commissions of inquiry and local government councillors and staff. All of these entities are subject to the provisions of the *Public Records Act 2002*, and most are subject to the provisions of the *Crime and Misconduct Act 2001.*

Public records: A public record is any form of recorded information, either received or created, that provides evidence of the decisions and actions of a public authority in carrying out its legislative, administrative or other public responsibilities.

Public records can be found in a number of different formats including but not limited to letters, minutes, memoranda, file notes, emails, web pages or blogs, social media postings such as 'tweets', maps or plans, photographs, drawings, audio or video recordings, as well as records stored in electronic business systems.

Risk factors

Poor records management practices can result in:

- Insufficient or inadequate recording of decisions
- Lost records
- Inappropriate destruction of records
- Inappropriate access to records.

This can expose your organisation to significant misconduct risks:

- Lack of proper protocols in relation to recordkeeping means that staff are less likely to understand the importance of recording their decision-making processes. This increases the potential for misconduct around decision-making and actions by public authorities.
- Inability of individuals to provide documentary evidence to account for their actions or decisions while carrying out duties as a public authority may cause damage to the reputation of both the organisation and staff members.
- Insufficient or inadequate documentary evidence in an organisation is likely to result in ineffective or poor decision-making.

- Projects or activities may be put at risk when decisions cannot be validated through access to documentary evidence.
- An absence of public records when an agency is seeking a court order may impact on its ability to provide a rationale for its position.
- Inappropriate access to records may be for personal gain or to cause detriment to other people or the organisation.

Misconduct offences

Inadequate management of public records can constitute misconduct or, depending on the circumstances, official misconduct. It can also result in dismissal and/or civil legal action against the individual and organisation involved. Consequences can include:

- Being charged and convicted of a criminal offence under the *Public Records Act 2002* if an individual unlawfully disposes of (including destroying, damaging, abandoning, transferring, donating, giving away or selling) a public record or any part of a public record.
- Being charged and convicted of a criminal office under the *Right to Information Act 2009* if an individual cannot, without reasonable excuse, produce the requested public records.

Strategies to prevent misconduct

Internal controls are essential to reduce the risk of inaccurate public records being created or public records being disposed of improperly. *Information Standard 40: Recordkeeping* and *Information Standard 31: Retention and disposal of public records* contain information on developing and implementing recordkeeping controls and protocols. Queensland State Archives can provide further guidance on strategies for developing and implementing these controls.

Policy development and promotion

- Develop recordkeeping policies and procedures which give clear guidance on records management requirements for employees. They should clearly state the obligations of staff in relation to creating, maintaining and disposing of public records.
- Adequately promote your organisation's code of conduct, policies, legislative obligations, retention and disposal schedule and other guidelines to staff. Ensure these are accessible.
- Ensure that staff receive initial and refresher training relating to recordkeeping, including maintaining confidentiality of public authority information.
- Clearly communicate any changes in public recordkeeping legislation, policies and procedures to all employees.
- Ensure that staff members are encouraged to report suspected official misconduct. Staff play a crucial role in reporting and preventing the illegal alteration, access, release or destruction of public records.

Security measures

The facilities, materials and methods of public records management must support their preservation for as long as they are needed to satisfy the accountability, legal, administrative and financial needs of the government. Preservation also assists the legitimate information needs of the community. Strategies should be put in place to protect records from unauthorised access, alteration, and accidental or intended damage or destruction. These may include:

- Establish effective and approved procedures for creating, maintaining and disposing of electronic public records.
- Ensure that staff place relevant public records on their designated Electronic Document and Records Management System (eDRMS).
- Ensure that there are adequate electronic security measures such as firewalls, anti-virus software and password access in place to prevent unauthorised access to public records.
- Ensure that all physical public records are securely stored at all times. Public records should be stored in a way that they are only accessed by those who require this information.
- Implement a business classification scheme for public records with corresponding security clearances.
- Ensure there are adequate procedures in place for employees who may be required to take records into a public area or to their private residence — e.g. requiring public records to be placed in a locked brief case when being taken outside of the office.
- Use a separation agreement that states the obligation of employees to maintain record confidentiality post separation.
- Immediately remove system access and other access tokens when employees, contract staff and third party service providers cease employment with your organisation.

Monitoring and compliance

- Make, maintain and protect all public records in accordance with the requirements of the *Public Records Act 2002*.
- Consider public record security breaches as a breach of your organisation's code of conduct. If such a breach amounts to official misconduct, refer it to the CMC and report lost or damaged records to Queensland State Archives.
- Ensure employees are aware of the consequences (disciplinary and legal action) related to failing to comply with record management policies, procedures and legislation.
- Ensure that regular audits on public records are conducted for the whole of the organisation. This is to ensure that staff are adequately recording their actions and decision making involved in performing their role as a public servant. This includes reviewing both electronic and hard copy files. Audits can include both internal and external audits.
- Ensure there is a good internal reporting system to help identify and prevent the illegal destruction of public records.
- Establish sound risk management strategies and practices, which encompass methods relating to identifying public record management risk areas.
- Record and report all actual and attempted breaches relating to public records.
- Promptly identify, report and rectify any weakness in protocols and procedures to prevent further breaches.
- Encourage self-assessment by employees in relation to their record management practices.
- Implement methods of monitoring any breaches of electronic security. Regularly review protection systems to identify any limitations in these systems in combating misconduct.

Disposal

- Do not dispose of any public record without authorisation from the State Archivist or other legal authority or excuse, as this is illegal under the *Public Records Act 2002*.
- Ensure that your organisation has a retention and disposal schedule approved by the State Archivist, and clearly communicate its requirements to all staff.
- In most circumstances public authorities can implement an approved retention and disposal schedule without further reference to the State Archivist. Public authorities should contact Queensland State Archives before implementing a records disposal program if it has been subject to a recent machinery of government change or if the records were created before 1950.
- Ensure that your organisation is compliant with the requirements of Queensland State Archives' Digitisation disposal policy before implementing any digitisation processes involving the destruction of original paper records.
- If authorisation is provided to dispose of the public record, ensure that an appropriate person properly destroys the record and that the disposal is documented in accordance with the requirements of *Information Standard 31: Retention and disposal of public records*.

Further information and resources

- Queensland State Archives & Crime and Misconduct Commission, *Managing public records responsibly* (PDF)
- Queensland State Archives & Crime and Misconduct Commission, *Retention and disposal of council record*
- Queensland State Archives, *Disposal freeze: a policy for Queensland Public Authorities*
- Queensland State Archives, *Digitisation disposal policy*
- Queensland State Archives, *Notification of lost public records*
- Queensland State Archives, *Application to dispose of damaged public records*
- *Public Records Act 2002*
- *Crime and Misconduct Act 2001*
- *Local Government Act 2009*
- *Right to Information Act 2009*
- *Code of Ethical Standards, Legislative Assembly of Queensland 2004*
- Right to Information Unit, Department of Justice and Attorney General
- Queensland Government, *Information Standard 31: Retention and disposal of public records*
- Queensland Government, *Information Standard 40: Recordkeeping*
- Queensland Ombudsman, *The good decision making guide*
- *Australian and International Standard 15489*
- Queensland State Archives website

Please contact us if you would like further detailed guidance and information on any aspect of this advisory.

Last updated: 16 April 2013

Contact us
Phone: (07) 3360 6060 or 1800 061 611 (toll-free in Queensland outside Brisbane)
Email: mailbox@cmc.qld.gov.au