Corporate Record Keeping

For flexible and remote working arrangements

April 2020

Given that many staff are transitioning to flexible working arrangements, normal lines of communication are becoming more complex. Staff may become more reliant on a combination of personal and corporate devices in order to continue business practices and communicate with colleagues. This increases the risk of records not being captured. The advice from Queensland State Archives on this matter is clear.

Public records in private accounts

Evidence of business activities are public records, regardless of how or where they are created or received, and must be managed in accordance with the *Public Records Act 2002* (the Act).

Public records include emails, social media interactions, text messages and messages in any other messaging applications, photographs and videos. The Act does not restrict the use of private email and social media accounts, messaging apps, or personal devices. However, public records created or received using these methods **must** be managed in accordance with the Act in the same way as public records created or received using official government channels.

Using private email and social media accounts and apps for work purposes can increase the risks of:

- public records not being captured, managed or accessible.
- public records being unlawfully destroyed or lost.
- information security being compromised (e.g. malware, information inadvertently shared).
- staff breaching other legislation, rules or guidelines (e.g. *Criminal Code Act 1899*, *Right to information Act 2009*, *Information Privacy Act 2009*, code of conduct).
- actual or perceived misconduct or corruption.

Responsibility for managing and capturing corporate records

All government employees need to be aware of their recordkeeping responsibilities under the Act to make and keep complete and reliable records of all work related interactions when using private accounts, apps and devices. This includes capturing any public record created or received in a private account or messaging app into an official government account **within 20 calendar days of creation or receipt**.

If you have any concerns or questions relating to this, please do not hesitate to contact the ERMT so that a solution can be provided during the current extraordinary circumstances. Corporate recordkeeping obligations as a MNHHS employee are summarised below to comply with the Act.

In summary, all staff are required to create, capture and appropriately manage records relating to their work, irrespective of the format of the records, and particularly records documenting decisions, approvals and actions taken.

Effectively, this means our staff:

- Must never destroy public records. Staff are only permitted to destroy *transitory* or short-term records as defined in the General Retention and Disposal Schedule (GRDS) or other approved Retention and Disposal Schedule.
- Must never store corporate records in personal portable storage devices.
- Must never use portable MNHHS storage devices for long-term storage of MNHHS records in lieu of the eDRMS or corporate network.
- Must, if they have relevant access, manage documents and records in MNHHS's approved recordkeeping system, eDRMS.