Office of the Information Commissioner
Queensland

Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Portable Storage Devices and Information Privacy

Portable Storage Devices (**PSDs**) are small, lightweight, easily transportable devices capable of storing and transferring digital data. Common PSDs include removable devices such as USB thumb drives or flash drives, rewritable CD/DVDs, memory cards and external hard drives and mobile devices with inbuilt storage such as tablets, laptops, and smartphones.

PSDs are capable of storing extremely large amounts of data.[1] Due to their portable nature and attractiveness, PSDs are susceptible to loss or theft. The potential damages arising from this risk increase if the PSD holds unsecured non-public data.

The *Information Privacy Act 2009* (Qld) (**IP Act**) requires agencies to ensure the personal information[2] they hold is protected against loss, unauthorised access, use, modification or disclosure and any other misuse.[3] Concerns about whether the agency's storage and security obligations have been met often goes hand-in-hand with privacy concerns about the secondary use of and disclosure of the accessed personal information.[4]

Risks of using PSDs

As noted, a common risk of using PSDs is that the device can be lost or stolen. Misuse, loss or unauthorised access, use, modification or disclosure of personal information can also arise through:

- a PSD infecting devices into which it is subsequently plugged with malware;
- insecure disposal of, or deletion of information from, PSDs; and/or
- unfettered access by third parties to the content of the PSD.

In addition, employees' use of personal PSDs to access, transfer or store agency data may increase the likelihood of a privacy breach. For example:

- the agency has less control over the use of security measures such as anti-virus and malware software, operating system and application updates and password, encryption and remote wipe capabilities

[1] For example, 1GB typically holds an average of 64,782 pages of Microsoft Word files. See https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf
[2] Personal information is any information about an individual who is or can reasonably be identified. See section 12 of the IP Act for the full definition.
[3] Information Privacy Principle (IPP) 4 for agencies other than health agencies and National Privacy Principle 4 (NPP) 4 for health agencies.
[4] IPP 11 for agencies; NPP 2 for health agencies.

- departing employees may accidently take away personal PSDs containing agency information; and
- unauthorised people are more likely to access personal PSDs at the employee's home, either inadvertently or by simply borrowing the device.

The damages arising out of a privacy breach involving a PSD increase where there is:

- no classification of information which may and may not be transferred to a PSD
- a lack of encryption or technical controls to protect data stored on the PSD
- no obligation to report loss or stolen PSDs; and/or
- a failure to promptly transfer agency records from the PSD to the agency network.

Legislation and policy obligations that impact on the use of PSDs

A number of laws and policies are relevant to the use of PSDs, including:

- *Public Records Act 2002* (Qld) governing recordkeeping for all Queensland public authorities.
- Information Standard 18: Information Security[5], which seeks to ensure a consistent, risk-based approach to the implementation of information security to maintain confidentiality, integrity and availability.
- Queensland Government Information Security Classification Framework (QGISCF)[6], which specifies a schema for the security classification of information and associated controls that reflect their classification level.
- Information Standard 38: Use of ICT Facilities and Devices[7], which aims to ensure the implementation of consistent policies in the management of employee use of and monitoring of information and communication technology (ICT) services, facilities and devices and that employees are aware of, understand and acknowledge their responsibilities when using ICT services, facilities and devices.

Managing the risk of using PSDs

A key strategy in minimising the risks of using PSDs is to develop and implement policies and procedures so that employees understand their obligations when using PSDs to access, store or transport agency data. Where possible, agencies should also use hardware and/or software controls to restrict or control the use of PSDs.

[5] Accessible at https://www.qgcio.qld.gov.au/documents/information-security-policy
[6] Accessible at https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf
[7] Accessible at https://www.qgcio.qld.gov.au/documents/use-of-ict-services,-facilities-and-devices-policy-is38

PSD policies and procedures should establish:

- What types of PSDs are permitted and under what circumstances? For example:
    - Will permission be granted to individual officers and/or given for a specific event or time period?
    - Who in the agency is authorised to grant permission to use PSDs and what is the process for requesting permission?
    - Whether agency-owned PSDs can be used for personal use and if so, are there are any conditions are placed on personal use?
    - What hardware or software security controls are to be used?[8]
- Whether personal PSDs are permitted and if so, what conditions are placed on their use. For example:
    - What types of PSDs will be considered and will it regulated by user type and/or job requirements?
    - Who in the agency is authorised to grant permission to use PSDs and what is the process for requesting permission?
    - Whether personal PSDs must have equivalent security standards to agency-owned devices?
    - In what circumstances can a PSD be shared? For example, are staff prohibited from installing file sharing apps on personal PSDs that will be used to hold agency data? Can staff share personal PSDs with agency data with non-staff or connect the device to an unsecured wireless network?
    - In what circumstances can a personal PSD be connected to the agency network or device?
    - Will employment cessation procedures include steps to verify that business information is removed from personal PSDs?
- How the rules surrounding use of PSDs interact with remote access to the network.
- Whether a central register of PSDs will be maintained and if so, what approved devices must be registered?
- What information may be transferred to a PSD and details of any additional safeguards appropriate to the security classification or value of the information. Where PSDs will store personal information, agencies should require that it be encrypted.
- What is considered acceptable use of PSDs for transport and storage of agency data, for example:
    - Agency data must remain on the device for the shortest practicable time.
    - Data should only be copied to the PSD, with the original files remaining with the agency.
    - Data is to be transferred to the agency network as soon as possible.
    - PSDs are to be used as transit media and not as long term or backup storage.

[8] For example, whether the PSD has password (or equivalent) locking functionality, that the password (or equivalent) must be enabled at all times, that the device has current malware protection and the capacity to be remotely located, remotely wipe data and securely erase files.

- How to securely erase data from PSDs.
- What to do with damaged or obsolete PSDs.
- What to do in case of lost or stolen PSDs or other suspected privacy breach.
- What processes are in place to audit or monitor compliance with PSD policies and procedures.
- Who employees can contact for advice on PSDs.

For additional information and assistance please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 9 January 2012 and Last Updated 18 April 2018

Changes to legislation after the update date are not included in this document