Document details

Security classification | PUBLIC
Date of review of security classification | 2013
Authority | Queensland State Archives
Author | Queensland State Archives
Document status | Final
Version | Version 1.0

Contact for enquiries
All enquiries regarding this document should be directed in the first instance to:

Government Recordkeeping Unit
Queensland State Archives
07 3131 7788
info@archives.qld.gov.au

Copyright
Recordkeeping implications of mobile and smart devices
Copyright © The State of Queensland (Department of Science, Information Technology, Innovation and the Arts) 2013

Licence

Recordkeeping implications of mobile and smart devices: A guideline for Queensland public authorities by Queensland State Archives is licensed under a Creative Commons Attribution 3.0 Australia Licence. To view a copy of this licence, please visit http://creativecommons.org/licenses/by/3.0/au/.

Information security
This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.
# Table of contents

1. **Introduction** ..........................................................................................................................4  
   1.1 Purpose ..........................................................................................................................  
   1.2 Audience .........................................................................................................................  
   1.3 Scope .................................................................................................................................  
   1.4 Authority ...........................................................................................................................  
   1.5 Policy framework .............................................................................................................  
   1.6 Definitions .........................................................................................................................  
   1.7 Acknowledgements ..........................................................................................................  

2. **Summary checklist** ..............................................................................................................6 

3. **Recordkeeping challenges posed by use of mobile and smart devices** .......................8  
   3.1 Identifying whether information contained on mobile and smart devices is a public record ...........................................................................................................  
   3.2 Capturing public records from mobile and smart devices into recordkeeping systems .............................................................................................................  
   3.3 Bring your own device and public records .....................................................................  
   3.4 Privacy .............................................................................................................................  
   3.5 Remote wipe and public records .......................................................................................  

4. **Strategies and solutions for managing the recordkeeping challenges posed by mobile and smart devices** .........................................................................................13  
   4.1 Overview of requirements for recordkeeping ....................................................................  
   4.2 Identification and capture of public records from mobile and smart devices ...................  
   4.3 Management solutions for mobile and smart devices ......................................................  
   4.4 Security considerations .....................................................................................................  
   4.5 Encryption of public records ............................................................................................  
   4.6 Reallocation and disposal of smart devices ......................................................................  
   4.7 Risk management considerations .....................................................................................  
   4.8 Summary ...........................................................................................................................  

*Appendix A: Glossary* ...................................................................................................................23 

*Appendix B: Overview of mobile and smart devices* .................................................................25 

*Appendix C: Risks to public records resulting from use of mobile and smart devices* ..........28 

*Appendix D: Decision matrix for identifying public records stored within mobile and smart devices* ..............................................................................................................................29 

*Appendix E: Guide to storage capacities for mobile and smart devices and related recordkeeping implications* ..................................................................................................................31
1. Introduction

1.1 Purpose

The purpose of this guideline is to assist public authorities meet their recordkeeping obligations under the Public Records Act 2002 where mobile and smart devices are used for business purposes.

The decision to allow official use of mobile and smart devices within public authorities should be based on a business need, as well as an assessment of potential risks associated with their use. This risk assessment would be likely based on the types of public records that the mobile and smart devices are likely to create, store, modify, use or transfer and the security classification of that information. Solutions, controls and associated business processes need to be regularly reviewed, as the pace of change in technology and user behaviour can generate new risks.

1.2 Audience

The intended target audience for this guideline includes:

- Chief Information Officers
- managers and staff responsible for records and information management within Queensland public authorities
- areas responsible for the planning and implementation of mobile and smart devices
- ICT staff responsible for the maintenance of public records created, captured, used and stored within mobile and smart devices.

1.3 Scope

The guideline outlines recordkeeping considerations arising from the use of mobile and smart devices within Queensland public authorities as defined in Schedule 2 of the Public Records Act 2002.

For the purposes of this guideline, mobile and smart devices are considered to be small, lightweight, portable devices which are capable of storing or transferring data, and can include a vast array of technologies such as smartphones, laptops and portable storage devices.

The guideline applies to mobile and smart devices that are being used for official government purposes, and which could be either supplied by a public authority or personally owned. Specifically the guideline provides advice on:

- key recordkeeping challenges posed by mobile and smart devices
- potential solutions to identified recordkeeping challenges, and
- risk management considerations associated with the use of mobile and smart devices within public authorities.

---

1 The Public Records Act 2002 covers all public records irrespective of the technology or medium used to generate the records. For more information on what is a public record, refer to the Queensland State Archives publication What is a Public Record, www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/what_is_public_record_200409.pdf
This guideline does not provide:

- implementation strategies for specific mobile and smart devices
- detailed technology-specific advice (e.g. security protocols, applications, hardware/software specifications etc.), or
- details on topics covered by existing Queensland State Archives’ advice (including the Guideline for Managing Closed Circuit Television (CCTV) Records or the Guideline for Managing Digital Photographic Images, Web 2.0 and social media considerations).

1.4 Authority

This guideline has been issued in accordance with section 25(1)(f) of the Public Records Act 2002, which enables the State Archivist to develop and publish policies, standards, and guidelines about the making, keeping, preserving, managing and disposing of public records.

1.5 Policy framework

Queensland State Archives is responsible for the provision of policy advice relating to a wide range of strategic recordkeeping and information management issues for Queensland public authorities. This guideline forms part of a wider recordkeeping policy framework that aims to promote best practice recordkeeping and information management within Queensland public authorities.

Public authorities must meet all legislative and regulatory requirements relating to the management of public records resulting from the use of mobile and smart devices, including those set out in the Public Records Act 2002 and associated information standards, Information Standard 40: Recordkeeping (IS40) and Information Standard 31: Retention and Disposal of Public Records (IS31).

A number of other legislative and regulatory requirements with recordkeeping implications apply to the use of mobile and smart devices. These include, but are not limited to, the Information Privacy Act 2009, Right to Information Act 2009, and Information Standard 18: Information Security. Specific obligations are expanded upon in more detail throughout this guideline where relevant. However the onus is on each public authority to make itself aware of other legislative and regulatory requirements which impact on its particular business operations.

1.6 Definitions

Records and information management specific terms are defined in Queensland State Archives’ Glossary of Archival and Recordkeeping Terms available on Queensland State Archives’ website.

A glossary providing clarification and definitions of terms used in this document relating to mobile and smart devices is included as Appendix A: Glossary.

1.7 Acknowledgements

A range of best practice information has been referenced in the development of this guideline, including advice published by the Office of the Information Commissioner Queensland, Public Record Office Victoria and the Office of the Victorian Privacy Commissioner.

Queensland State Archives acknowledges the many public authorities that contributed to the development of the guideline.

2. Summary checklist

The following checklist provides a summary of the key recordkeeping considerations associated with the use of mobile and smart devices, and the relevant section of the guideline where each key recordkeeping consideration has been addressed.

<table>
<thead>
<tr>
<th>Checklist of criteria to consider in managing the recordkeeping implications of mobile and smart devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification, capture and retention of public records</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Personal devices (BYOD)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Privacy</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
| **Remote wipe** | • Have the recordkeeping implications of remote wipe functionality been considered?  
• Are incident response procedures for lost or stolen mobile and smart devices documented? | See section 3.5 |
| **Staff training and awareness** | • Are staff aware of the risks associated with the use of mobile and smart devices?  
• Are expectations associated with use of mobile and smart devices actively promoted, via both formal training activities and informal communication mechanisms?  
• Have other legislative and policy obligations impacting on the use of mobile and smart devices been considered? | See section 4.1 |
| **Software and hardware controls** | • Have hardware and software controls been considered and implemented for the types of mobile and smart devices in use, in accordance with their own risk assessments, policies and procedures, and relevant recordkeeping, privacy and security requirements? | See section 4.3 |
| **Security considerations** | • Have required security solutions been identified based on types of mobile and smart devices used?  
• Have categories of information and associated circumstances for permitted use on mobile and smart devices been identified?  
• Has consideration been given to any need to differentiate between different categories of users accessing public records and public authority networks via mobile and smart devices? | See section 4.4 |
| **Encryption** | • If encryption is permitted as a strategy for safeguarding public records held on mobile and smart devices, is its use clearly explained (e.g. in policy or procedures)? | See section 4.5 |
| **Disposal and reallocation** | • Have the issues associated with the secure deletion of public records from mobile and smart devices before disposal or reallocation been considered? | See section 4.6 |
| **Risk assessment** | • Has an appropriate risk assessment for the use of mobile and smart devices been conducted, in line with relevant requirements such as recordkeeping, privacy and security? | See section 4.7 |
| **Storage of public records** | • Have consequences relating to the controls for the storage of information captured on mobile and smart devices (including USB and external hard drive storage) been considered?  
• Are the recordkeeping implications of cloud computing also considered for the storage of public records? | See Appendix E |
3. Recordkeeping challenges posed by use of mobile and smart devices

The use of mobile and smart devices has increased significantly over recent years, and is likely to continue to do so for some time. The physical size and cost of many mobile and smart devices has decreased, while storage capacity has increased. Mobile and smart devices are rapidly evolving, easy to use and convenient to carry, providing public sector employees with the potential to create, store and access certain government information anywhere, anytime. Devices may be relatively cheap (e.g. USB keys), widely owned by individuals (e.g. smartphones), and much harder to detect because of their small size. An added feature of compact mobile and smart devices is that they can be easy to lose or misplace. For a general overview of mobile and smart devices in the context of this guideline, refer to Appendix B.

The rapid evolution and adoption of mobile and smart devices, whether government supplied or bring your own device (BYOD – see section 3.3), creates a number of records management challenges and risks for public authorities.

For example, due to the increased use of mobile devices (e.g. from USB keys to smartphones and tablets), public records which traditionally were created in the office or fixed location now have the potential to be created anywhere, any time (e.g. in the home of a patient, in the field while taking water samples etc.). The use of these devices means that public records have an increased potential to be created and carried in unrestricted environments, outside of the control and integration with corporate recordkeeping systems.

The integrity of public records should not be compromised as a result of the use of mobile and smart devices (e.g. by not capturing records from mobile devices into recordkeeping systems, through to the alteration or unlawful disposal of public records). Section 4.7 provides advice on managing the risks associated with use of mobile and smart devices and public records.

For example

The main recordkeeping challenge associated with use of mobile and smart devices will be likely associated with the capture of public records created on mobile and smart devices. However, recordkeeping considerations will also need to be identified for users of mobile devices who access, view or download public records from internal systems.

For example, users who copy to and edit documents on a mobile and smart device must then reintroduce these documents back into the public authority’s recordkeeping system. An added complexity relates to information contained within applications specific to mobile and smart devices which may be difficult to integrate into a public authority’s recordkeeping system. Further information relating to the recordkeeping risks associated with mobile and smart devices are outlined in Appendix C.
The following section of the guideline provides an overview of the recordkeeping challenges which are associated with the use of mobile and smart devices.

3.1 Identifying whether information contained on mobile and smart devices is a public record

Not all information that is created or stored on mobile and smart devices is a public record. Information about personal or non-business transactions and copies of existing public records are examples of ephemeral items that do not need to be managed as public records but should still be subject to organisational policy and procedures to ensure they are managed appropriately (e.g. in accordance with privacy requirements). Refer to Appendix D for a decision matrix to assist in determining whether information contained within mobile and smart devices could be identified as a public record.

To identify whether a mobile and smart device contains public records, consideration should be given to what records need to be kept of the business being transacted, and how these records will be managed as part of the public authority’s broader recordkeeping framework. As with public records in all formats, information held on mobile and smart devices that document business activity and are not captured elsewhere, are required to be captured and stored in a public authority’s recordkeeping system.

3.2 Capturing public records from mobile and smart devices into recordkeeping systems

As more data is created, sent and stored on mobile devices, the level of risk related to the lack of capture and maintenance of public records grows in several ways, including:

- Physical loss of devices increases the likelihood of corruption of records, privacy breach, loss of intellectual property and other related problems. If public records which are stored on mobile or smart devices (and have not been captured in a public authority’s recordkeeping system) are lost irretrievably, notification to the State Archivist must be made through completion of a Notification of lost public records form.

- Knowing what records are available (and accessible, to ensure sufficiency of searches) on mobile devices becomes more difficult. This is particularly problematic for legal counsel and others that must assess the information that the organisation has available to it, within legislative timeframes, during e-discovery, early case assessment and similar types of litigation-related activities, as well as Right to Information applications.

- The growing number of devices accessing public authority networks – as well as home networks, publicly available Wi-Fi networks etc. – increases the likelihood of malware or other intrusions entering the corporate ICT network, potentially resulting in loss of data.

---

5 Under section 13 of the Public Records Act 2002, the disposal of public records must be authorised by the State Archivist. Authorisation to destroy public records is usually granted through an approved Retention and Disposal Schedule. However where public records have been lost, the State Archivist should be notified by completing and submitting the Notification of lost public records form, www.archives.qld.gov.au/Recordkeeping/Disaster/Pages/Default.aspx
If information held on mobile and smart devices has been identified as a public record, strategies will need to be developed to capture these records into a public authority’s recordkeeping system. Due to the diverse nature of the information potentially residing on mobile and smart devices, there is a risk that public records may not always be transferred to a recordkeeping system at the time of creation or receipt. Lack of capture may be a result of a number of factors, including:

- a user’s lack of awareness of their recordkeeping responsibilities such as not understanding what a public record is within the context of mobile and smart devices
- lack of recordkeeping guidance provided by a public authority to its users of mobile and smart devices
- poor network access, or
- devices not compatible with remote access to a public authority’s recordkeeping system.

In order for public records to be captured, transferred to a public authority’s recordkeeping system and retained appropriately, users of mobile and smart devices must first be able to identify whether information on their device is a public record, and then transfer the records into the corporate system in a timely manner.

### For example

Devices such as tablets and smartphones may typically be used to access work emails while away from the office. This functionality allows users to carry out a number of tasks, including the ability to view, create, send and delete emails. Regardless of access mechanism, normal recordkeeping procedures should be adhered to. For example, emails identified as a public record should not be deleted until they have been captured into a public authority’s recordkeeping system. If the mobile and smart device being used to remotely access work emails does not have access to the public authority’s recordkeeping system, those emails identified as a public records should not be deleted until such time as they have been captured into a recordkeeping system.

The increasing storage capacities of mobile and smart devices pose a number of recordkeeping challenges for public authorities. A guide to the storage capabilities of mobile and smart devices and associated recordkeeping implications are outlined in Appendix E.

### 3.3 Bring your own device and public records

The rapid adoption of mobile and smart devices has led to many public authorities allowing employees to use their own personal smartphones, tablets and other devices for business purposes – also called ‘bring your own device’ (BYOD). Allowing employees to use privately owned devices for official business has the potential to result in a reduction in costs in both procurement and management of mobile and smart devices. However, the implementation of BYOD poses many recordkeeping related risks that need to be addressed, including:

- the potential for information to be held on a wide range of devices (as outlined in Appendix B)
- lack of control of information and the device (including security and access requirements from the perspective of the public authority)
  - e.g. possibility of employees not using their own devices under a formalised agreement, and
- capture of public records created and stored on devices into recordkeeping systems.
Key point

Use of BYOD may vary across a public authority depending on the user’s needs. For example, some may require devices to frequently access sensitive data; others may require devices to access corporate data while at external business meetings; others may require devices because their work is largely mobile; or others may require a BYOD remote access to accommodate occasional work away from their desks.

The introduction of employee-owned devices can raise a different set of expectations about the level of control a public authority can exert over the devices and the level of access the devices have to organisational information. The balance point between control and flexibility in the management of employee-owned devices will be different to public authority-supplied devices.

Decisions may need to be made in determining whether the mobile and smart device was used for personal or business purposes (especially in cases where the device is owned by the individual as opposed to the public authority). Where devices are owned by the individual, there may be some risk that not all public records will be captured. For those records which are captured, characteristics required for full and accurate records will need to be met.

Key point

The capture of public records from mobile and smart devices can be complicated due to the perceived ‘personal’ nature of the devices. For example, a device supplied by a public authority may be managed differently to a personally-owned device.

Regardless of ownership, staff should be made aware that if a device (e.g. whether a personal USB key or government supplied tablet) contains public records, ownership of the public record resides with the public authority, and should be managed in the public authority’s recordkeeping system.

3.4 Privacy

The use of mobile and smart devices has significant potential for privacy implications. Public authorities may need to produce information stored on mobile and smart devices (e.g. when claims arise which require information that is created or stored on mobile and smart devices to be produced because it is relevant to the claim). Public authorities need to be aware of their obligations under the Information Privacy Act 2009. The information privacy principles set out in the Information Privacy Act 2009 include obligations to appropriately protect and secure personal information, to ensure it is not improperly or unlawfully accessed, used or disclosed. These obligations apply to public authority’s use and management of mobile and smart devices. A failure to meet these obligations could result in not only a breach of the privacy principles for storage and security of personal information, but also those which prohibit disclosure of personal information.6

---

3.5 Remote wipe and public records

Remote wipe is a feature that can be installed on many network connected mobile and smart devices. This feature can be an effective method for preventing data from being compromised on devices which may be lost or stolen. However, remote wipe also has recordkeeping implications, specifically the potential loss of any public records on the mobile or smart device which have not yet been captured into a public authority's recordkeeping system.

Any mobile or smart device that is lost or stolen and contains public records not captured within a public authority’s recordkeeping system will require the public authority to submit a Notification of lost public records form to Queensland State Archives to advise them of the loss.

A notable limitation related to the remote wipe procedure is that on some platforms, removable media such as memory cards are not erased by the remote wipe function. In addition, remote wipe cannot be activated unless the mobile or smart device has a data connection over a Wi-Fi, cellular or satellite signal.

---

4. Strategies and solutions for managing the recordkeeping challenges posed by mobile and smart devices

The following section of the guideline provides an overview of various strategies and solutions public authorities may consider in order to manage the recordkeeping challenges associated with the use of mobile and smart devices as highlighted in section 3.

4.1 Overview of requirements for recordkeeping

The recordkeeping requirements associated with information contained on mobile and smart devices are not unique to these devices. The Public Records Act 2002 states that public records are not defined by format. A public record is information in any format, either created or received, required as evidence of the business activities of a public authority.

Not all information that is created or stored on mobile and smart devices will be a public record. Information about personal or non-business transactions and copies of existing public records are examples of ephemeral items that do not need to be managed as public records but may still be subject to organisational policy and procedures to ensure they are managed appropriately (e.g. in accordance with privacy requirements).

Regardless of device, the responsibility for ensuring any public records that may be created, received or stored on mobile and smart devices still primarily resides with the user of the device.

The recordkeeping requirements outlined by the Public Records Act 2002, together with the core principles of Information Standard 31: Retention and Disposal of Public Records (IS31) and Information Standard 40: Recordkeeping (IS40), apply regardless of format or technology used. However, meeting the recordkeeping requirements associated with employee use of mobile and smart devices does differ from more traditional recordkeeping practices due to the technical and procedural challenges posed by the diverse nature of the technologies.

It is recommended that public authorities create or update policies that include recordkeeping obligations associated with the use of mobile and smart devices. In addition to recordkeeping obligations, policies and procedures on the use of mobile and smart devices should also include information on a range of topics including (but not limited to) information privacy (see section 3.4) and information security requirements (see section 4.4).
4.2 Identification and capture of public records from mobile and smart devices

In order to capture public records from mobile and smart devices into existing recordkeeping processes, public authorities may need to consider implementing a combination of technical and procedural solutions.

- Technical solutions will likely focus on systems to assist the capture of public records created and stored on mobile and smart devices into organisational recordkeeping systems.
- Procedural solutions will tend to focus on ensuring users are aware of the need for full and accurate public records, and methods to capture any public records that are created and stored on mobile and smart devices into a public authority’s recordkeeping system.

Due to the diversity and frequent release of new devices, public authorities will need to continually review and re-evaluate the recordkeeping solutions developed for mobile and smart devices. Training should also be provided to ensure staff are kept aware of their recordkeeping responsibilities and obligations.

In addition to considering the recordkeeping specific requirements outlined in IS40 and IS31, policy and procedures for mobile and smart devices should also consider the typical functionality employed on these devices which present potential recordkeeping challenges.

The following checklist provides a number of statements which may assist in identifying whether information contained within mobile and smart devices should be captured as public records.

**Checklist**

Mobile and smart devices may contain public records if one or more of the following apply:

- they contain information applicable to the purpose and works of the public authority that is unique and not available anywhere else (e.g. not duplicated from websites or recordkeeping systems)
- they contain a primary source of evidence of a public authority’s actions, policies, business, decisions, mission, etc.
- they are used in relation to the public authority’s work and generate evidence of work (e.g. notes added to meeting minutes, photographs taken to document damaged roads)
- their use is authorised by the public authority
- they contain information that is required as a business need.

In addition to this checklist, Appendix D contains a decision matrix to assist in identifying whether information contained on mobile and smart devices could be identified as a public record.

If information contained within mobile and smart devices is identified as a public record, the approach taken by public authorities to capture these public records into public authority
Recordkeeping systems will likely vary depending on the context and format of the information. For example, a public authority may develop business processes which dictate that text messages received or sent from smartphones can be captured via file notes. Alternatively, photographs taken during the construction of a building may be required to be captured in their original format.

The decisions taken as to how public records are captured from mobile and smart devices should be proportionate to the extent and purpose of use of the public records in a public authority. For example:

- public records documenting high risk activities will require more detailed information to be captured, and more likely in their original format
- public records documenting lower risk activities such as routine announcements may be sufficiently captured by a log of messages sent, including date and time.

Decisions regarding appropriate methods of capture of public records from mobile and smart devices should be documented in organisational policies and/or procedures.

### For example

A business email that is a public record sent from a personal mobile and smart device to a client will need to be captured into a public authority’s recordkeeping system. However, a personal tweet or text message sent from the same mobile or smart device may not need to be captured in the same way.

Capture methods may include:

- a file note of a text message
- connecting the device to a PC to download the file and print to capture into a public authority’s hardcopy recordkeeping system
- connecting the device to a PC to download the file and capture into a public authority’s electronic document and records management system (eDRMS)
- third party capture software
- enabling capture techniques specific to applications (e.g. option available with email applications to ‘leave a copy on the server’).

Enforcing the access requirements of a public authority for the identification or capture of public records from mobile and smart devices may be difficult (more so with employee-owned devices). Effective tools to help enforce access requirements may include ensuring users of mobile and smart devices such as tablets and smart phones (whether BYOD or government supplied) sign permission of use forms requiring user acceptance and signature for mobile and smart device use within their public authority. These forms could outline policy requirements such as:

- expectations of the employee with regards to processes to manage any public records stored on a mobile and smart device
- authorised actions of the public authority (e.g. situations where the public authority may need to access the device and the information contained within)
- legal issues that may require consideration (e.g. confidentiality, privacy and liability).

---

4.3 Management solutions for mobile and smart devices

Potential solutions available for the management of ‘active’ mobile and smart device (e.g. smartphones and tablets) access to public records include:

- installation of mobile device management software (specifically applicable to government supplied devices, see section 4.3.1)
- use of virtualisation technologies (suited to both government supplied and BYOD devices, see section 4.3.2).

If mixed device ownership is allowed (i.e. BYOD and government supplied), then policy consideration should be given to which, if any, differences in access to information and services are appropriate. In some cases this could involve the use of applications to separate public authority records from personal information. There may also be differences in the level of technical support provided (if any) between public authority owned devices and employee owned devices.

4.3.1 Use of mobile device management software

Mobile device management (MDM) software gives administrators the ability to centrally configure, manage and secure applicable mobile and smart devices (e.g. smartphones and tablets). As a result, MDM software provides public authorities with a host of policy options for helping to secure the information contained within mobile devices on multiple platforms, running different versions of different operating systems.

From a recordkeeping perspective, MDM software should enable the management of corporate information on or accessible from mobile and smart devices. There are a number of important recordkeeping features that should be carefully considered and discussed with a public authority’s IT area if any MDM solution is implemented. These include (but are not limited to):

- Integration with public authority networks and/or systems
  - This capability will allow those public records that are created or stored on a mobile and smart device to be transferred to corporate recordkeeping systems, ensuring information is managed in accordance with the recordkeeping requirements of the Public Records Act 2002 and IS40 and IS31.

- Ability to dictate which groups of users have access to different types of information, networks and applications
  - This functionality is typically based on users’ roles and responsibilities within a public authority.

- Potential to remotely wipe information from a mobile and smart device
  - Mobile device management solutions typically contain the ability to selectively wipe data (e.g. through isolating work information from personal information, a public authority's IT area can wipe work information from a personal device without wiping personal information or vice versa10). From a recordkeeping perspective, public authorities may prefer to investigate potential capability to ‘lock’ devices as opposed to wiping information in the first instance.

---

9 Refer to Appendix B for more information relating to passive and active mobile and smart devices.
10 This is particularly desirable from the point of view of being able to destroy records which are stolen, lost or are taken by former employees. Relevant recordkeeping and privacy considerations should be taken into account prior to any remote wipe procedure.
Key point

Policies for the use of mobile and smart devices should outline various recordkeeping responsibilities including how often users are required to transfer any public records from a device to corporate networks. For example, if a mobile and smart device is used to take notes of a meeting, these notes should be transferred and captured (e.g. as a file note) into a public authority’s recordkeeping system before they can be deleted from the mobile and smart device.

4.3.2 Use of virtualisation technologies

An alternate solution to an implementation of MDM software may be to allow users to work in virtual environments, through use of virtualisation or ‘thin client’ solutions. This solution may also be more suited to use of BYOD.

Virtualisation allows users of applicable mobile and smart devices to access the systems and servers they would normally access at their desk through desktop and application virtualisation technologies and terminal servers. In order to achieve this, virtual desktops are hosted on a remote server and emulate a desktop computer to provide access to IT services, including applications and tools users need to do their job.

Through the use of a thin client such as Citrix, users run their applications and access network resources in a Citrix session, in essence using the mobile device as a viewer. The benefit of this approach is that there is no requirement for the data to leave the server and be transferred to the user’s device. Virtualisation helps to prevent data loss as information is not stored on mobile and smart devices while still allowing users to access corporate applications and network resources.

Virtualisation does not however protect against loss of public records which have been created on mobile and smart devices and not subsequently transferred to a public authority’s recordkeeping system.

While use of thin client technology has the potential for a number of benefits, there are a number of prerequisites for use, including connectivity to the host server.

While allowing users access to thin client technology goes some way to protecting public records in terms of loss or theft of a mobile and smart device, it may only be a partial solution and should be implemented in conjunction with other protections, such as endpoint security. Depending on purpose of use, public authorities intending to implement Citrix-based solutions may need to consider the following security features:

- access to the clipboard could be disabled to prevent users from being able to copy and paste data from their Citrix session to their device
- local drive mapping could be disabled, preventing users from saving data from the Citrix session to local drives on the device
- local port mapping (such as serial ports and memory card ports) could be disabled, and
- restrictions on locally attached printing so that users cannot print to certain devices.

---

11 A thin client is a computing device or program that relies on another device for computational power
13 Portable Storage Devices, privacy survey, December 2011, Office of the Victorian Privacy Commissioner
Solutions implemented by public authorities will depend on the purpose of use and type of public records to be accessed by mobile and smart devices. Public authorities need only take reasonable steps where required to ensure information is protected.

**Key point**

It is important to note that Citrix will not prevent a device from accessing shared drives locally in the conventional manner. If the device has access to network drive shares outside of Citrix, data could still be copied to the local machine, including to removable media (i.e. memory cards or other mobile and smart devices) unless other measures are taken to prevent this. Also note that there is not a reliable method to prevent print screen or other screen capturing software from capturing data directly off the screen. For example, an iPad can capture screen content without any additional software.14

4.3.3 Implementation of management solutions for mobile and smart devices

As previously identified, implementation of management solutions for ‘active’ mobile and smart devices may serve a number of purposes, including to:

- enforce organisational policy on applicable mobile and smart devices
- manage the mobile and smart devices themselves, and
- ensure data on devices is monitored, transferred and otherwise managed in accordance with required policies.15

Records managers should consult with their ICT areas to ensure relevant recordkeeping considerations can be incorporated into any solution before deciding on particular software, hardware, access and other controls (including permission of use forms requiring users acceptance and signature) for mobile and smart devices used within their public authority.

**Key point**

Mobile and smart device management solutions need not be complicated. For example, users should be educated about appropriate password application. Following good practice security and network procedures can help protect public records contained within mobile and smart devices. Mobile and smart devices such as tablets and smartphones should require a password containing uppercase / lowercase letter, numbers and special characters rather than simple passcodes (e.g. four digit passcodes).

---


4.4 Security considerations

As a result of the use of mobile and smart devices (particularly in relation to BYOD), there are many security considerations related to public records which must be addressed. These include:

- ensuring only authorised persons access public authority networks
- only authorised devices access public authority networks, and
- public authority networks are secure and compatible with mobile device use (e.g. security of information transfer).

Security features and capabilities employed will vary depending on the mobile and smart devices in use, the type (and classification) of information to be accessed, and the purpose for the deployment of devices. Controls over the use of mobile and smart devices (including controls implemented on public authority networks) should be commensurate to the value of the information stored on the device.

The Defence Signals Directorate\(^{16}\) states that when setting up a secure system which uses mobile devices, a combination of controls may be required to ensure the validity of the solution. The security posture of devices can be progressively improved by combinations of capabilities as shown below in Figure 1\(^ {17}\).

---


\(^{17}\) For more detailed information relating to enabling the security features identified above, refer to the Defence Signals Directorate advice.
The Queensland Government Information Security Classification Framework\textsuperscript{18} should be considered to determine the level of security that should be applied to different levels of information classification. According to this framework, public authority policies and related procedures should clearly explain and define to users the categories of data which are permissible for use, and in what circumstances. These include:

- when corporate mobile and smart devices may be used for personal use
- which data cannot be stored on unencrypted mobile and smart devices, and if not, whether encrypted mobile and smart devices may be used
- whether users may share the use of corporate mobile and smart devices. Note that this runs the additional risk of private and personal information being seen by others
- when to transfer information to organisational recordkeeping systems, and
- when appropriate to delete, or digitally wipe data from devices in their possession.

The only certain way to prevent theft or loss of sensitive public records (e.g. those classified ‘IN-CONFIDENCE or above) from a mobile or smart device is to completely prevent such information from being accessed on a mobile or smart device. While the trend towards use of mobile and smart devices includes more mobile access to information, public authorities should look to classify their public records according to the Queensland Government Information Security Classification Framework\textsuperscript{19}. Once information is classified to the security framework, acceptable access and use policies should be defined according to the relevant security classifications.

**Key point**

If a public record were to have major negative consequences if lost or intercepted, these records (or copies of) should not be stored on a mobile or smart device without adequate security controls or transmitted across unsecured networks.

Risk assessments should be undertaken to identify the highest security classification that is able to be accessed by mobile and smart devices. This will vary depending on public authority specific circumstances and requirements. For example, additional security and network access rights may need to be considered for mobile and smart devices that have data storage as a secondary function (for example, MP3 players, iPods, and digital cameras). Public authorities should consider relevant standards such as Information Standard 18: Information Security\textsuperscript{20} as an example of best practice to inform their decision-making processes for these types of devices. For example, a public authority may determine that mobile devices which have data storage as a secondary function should only allow the one way transfer of information from the device to the network.

This guideline is simply intended to provide an overview of some of the security features and capabilities which may be required for use of mobile and smart devices rather than detail specific implementation advice for specific security considerations.


4.5 Encryption of public records

Public authorities may identify risks associated with the storage of certain public records (e.g. those records containing personal or sensitive information) on mobile and smart devices. Where this risk is identified, encryption is one of many options available to public authorities to manage sensitive public records.

Encryption is the process of systematically encoding data before transmission and during storage, so that an unauthorised party cannot easily decipher the data. Public authorities should consider how encryption can be enforced on mobile and smart devices by system administrators. Keeping public records in encrypted form increases the risk of not preserving the records in a readable and accessible format over the time they are required to be kept.


4.6 Reallocation and disposal of smart devices

Public authorities should ensure that mobile and smart devices are only reallocated or disposed of once any public records stored on the device have been transferred to the public authority’s recordkeeping system, and corporate information deleted or digitally wiped. When mobile and smart devices are deemed obsolete, or the employee no longer requires use of the device (e.g. through resignation, etc.), a suitable disposal regime should be developed which, in some circumstances, may include outright destruction. Refer to the Queensland State Archives publication Advice on the destruction of public records23 or alternatively, the State Records Office of Western Australian guideline Sanitising digital media and devices24 for further information on the destruction of electronic records and devices.

4.7 Risk management considerations

Recordkeeping risks resulting from the use of mobile and smart devices can be grouped broadly into the categories of data theft / loss and compromises in the security of information (refer to Appendix C for detailed examples). Policies and procedures relating to mobile and smart device use should reflect the risk profile of the public authority. When examining the risk profile of a public authority, the potential information to be accessed, created and stored on the mobile and smart device should be taken into consideration. The following checklist provides examples of a number of factors that should be considered when undertaking a risk assessment of mobile and smart devices.

22 The Queensland Government Enterprise Architecture (QGEA) is a collection of ICT policies and related standards and guidelines developed to guide agencies in their information communication technology operations and management, www.qgcio.qld.gov.au/products/about-the-qgea
4.8 Summary

If mobile and smart devices are used within a public authority to access organisational resources, the public authority should consider the associated recordkeeping implications by:

- developing policies and/or procedures outlining
  - user recordkeeping responsibilities, including outlining responsibilities for the identification and capture of public records into public authority recordkeeping systems as soon as practicably possible, and
  - any functional restrictions, such as device modifications or installation of applications.

- ensuring that only certain devices upon which security controls can be enforced, such as encryption and remote wipe, are permitted on government networks

- considering differences in access and support considerations for government supplied devices compared to BYOD

- considering how (or if) data is synchronised across devices, ensuring that sensitive or personal public records are not stored insecurely in the cloud (see Appendix E for more information relating to cloud) or on the device.25

25 Office of the Victorian Privacy Commissioner
Appendix A: Glossary

Records and information management specific terms are defined in Queensland State Archives’ Glossary of Archival and Recordkeeping Terms available on Queensland State Archives’ website.26

**Bring your own device (BYOD)** - BYOD is a concept that allows employees to make use of their personally-owned or government supplied technology devices to stay connected to, create, or access data from, or complete tasks for their public authority. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices.

**Encryption** - Encryption is the process of systemically encoding data before transmission and during storage so that an unauthorised party cannot decipher it. Distinction should be made between hardware-based and software-based encryption. Hardware-based encryption is forced on the user; whereas software-based encryption gives the user the choice of whether to do so or not.27

**Gigabyte** - A gigabyte is 1024 megabytes.

**Malware** – Short for malicious software, malware is software designed to infiltrate or damage a computer system, without the user’s consent.

**Sanitising media** - The process of erasing or overwriting data stored on media.

**Mobile device management (MDM)** – MDM software secures, monitors, manages and supports mobile devices deployed across an organisation.

**MP3** - MPEG-1 Audio Layer 3 is a popular digital audio encoding and compression format.

**Operating system (OS)** - The software that supports a device’s basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

**Personal Data Assistant (PDA)** - A small, mobile, hand-held device which provides computing and data storage/retrieval capabilities for personal and business use.

**Portable storage device** - Also known as ‘removable storage device’. A small, lightweight, portable, easy to use device, capable of storing and transferring large volumes of data. They are either exclusively used for data storage (e.g. USB keys) or are capable of multiple other functions (e.g. iPods; PDAs).

**Portable external hard drive** - Portable and typically self-powered, they operate on a plug-and-play basis. Any computer with USB or FireWire capability will recognise the external hard drive as a storage device, which can then be accessed like a normal internal hard drive, making it easy to transfer large files.28

---

27 Portable Storage Devices, privacy survey, December 2011, Office of the Victorian Privacy Commissioner
28 Portable Storage Devices, privacy survey, December 2011, Office of the Victorian Privacy Commissioner
Remote access - Access to a system that originates from outside an agency network and enters the network through an Internet gateway.

Removable media - Storage media that can be easily removed from a system and is designed for removal.

Smartphone - A mobile telephone with built-in applications and Internet access. In addition to their built-in functions, smartphones can run a vast array of third party applications, turning the once single-minded mobile phone into a mobile computer.

Tablet - Since early 2010, new tablet computers have been introduced with mobile operating systems and represent a new type of computing device. These devices are normally touch driven and most frequently use screens with multi-touch capabilities. The Apple iPad has been the most prominent to date, but the market is broadening. A significant trait of tablet computers is that the main source of third party software for these devices is typically through online distribution.

Terabyte - A terabyte is 1024 gigabytes.

Thin client - A client terminal or personal computer that relies on the server to perform the data processing. The ‘thin client’ software is used to send keyboard and mouse input to the server and receive screen output in return. The thin client does not process any data; it processes only the user interface. The benefits of improved maintenance and security (due to central administration) and low bandwidth requirements make it ideal for devices. A widely used thin client is Citrix.29

USB - Universal Serial Bus (USB) is a widely used interface for attaching devices to a host computer. Personal computers and laptops have multiple USB ports which enable many devices to be connected using a single standardised interface socket. Devices can be connected and disconnected without rebooting the computer or turning off the device.

USB key - Also known as “flash drive”, “USB stick”, “memory key”, “USB drive”. A device that plugs into the computer’s USB port. Small enough to hook onto a key-ring, it allows data to be easily downloaded.

Wireless/Wi-Fi - Wireless communication describes telecommunications in which electromagnetic waves rather than wire carry the signal over part or the entire communication path. Personal computers are increasingly connecting through wireless means, as opposed to the traditional ‘wired’ means.

29 Portable Storage Devices, privacy survey, December 2011, Office of the Victorian Privacy Commissioner
Appendix B: Overview of mobile and smart devices

While devices such as USB keys and laptops have been used by public authorities for a number of years, newer types of mobile and smart devices are increasingly being used as both corporate and personal devices.

A mobile and smart device is a small, lightweight, portable device which is capable of creating, accessing, storing or transferring data, and can include a vast array of technologies, including (but not limited to):

- smartphones, tablets and Personal Data Assistants (PDAs)
- laptops
- external storage devices (e.g. portable external hard drives)
- portable flash memory (e.g. USB keys / memory cards)
- devices with inbuilt accessible storage (e.g. MP3 players, iPods).

The use of mobile and smart devices within a public authority offers a number of advantages including greater accessibility, mobility, convenience and efficiency of access to public records. Mobile and smart devices have allowed users to progressively move away from paper-based environments.

Mobile and smart devices such as tablets and smartphones contain internal memory typically ranging from 8 to 64 gigabytes\(^\text{30}\). Today, many people carry with them at least one mobile and smart device capable of capturing and storing public authority records. These devices also allow the installation of applications which, if not managed or properly controlled, have the potential to cause security and privacy implications for government ICT systems and networks.

In addition to the broad range of mobile and smart devices available, devices such as smartphones may operate over a variety of platforms or operating systems, including (but not limited to):

- Google / Android
- Apple / iOS
- RIM / BlackBerry
- Symbian
- Windows.

Further, not only are there multiple platforms, each individual operating system may contain a number of variations as new versions are constantly developed. Added to the variations in operating systems within devices, public authorities are likely to have a number of different mobile devices in use simultaneously (whether authorised or otherwise). The variation in use associated with a diverse range of mobile and smart devices creates a number of recordkeeping, privacy and security challenges. These challenges are expanded upon in more detail throughout this guideline.

\(^{30}\) Refer to Appendix E which provides a guide to the storage capabilities of various mobile and smart devices.
For example

Users who upgrade frequently to the latest model of tablet/smartphone, put pressure on administrators to constantly test and integrate new models into an organisation’s operating environment of internal sites, applications, domain access, networks etc. Given that there are fragmentation issues even within the same operating platform (e.g. the variety of Android-based devices by different hardware manufacturers, and differences between the versions of Apple’s iOS), each new device represents differing risks and challenges for administrators. Security related updates and fixes should be prioritised according to risk and these may demand more frequent and timely application for the protection of the public authority.

The following diagram (Figure 2) from the Australian Government Information Management Office (AGIMO)\(^3\) categorises mobile and smart devices on a continuum according to their intrinsic capability:

![Categorisation of mobile and smart technology devices](image)

The devices shown in Figure 2 range in capabilities from passive devices that do not have any complex processing or intercommunications capability on their own (e.g. memory cards), to devices that have intrinsic programming logic and are able to perform some processing and communications tasks independent from other devices (e.g. smartphones).

**Passive mobile and smart devices**

Examples of passive mobile and smart devices include:

- USB drives
- data card readers and data cards.

---

Passive devices, while not containing any information creation capabilities, have the potential to store significant amounts of public authority information (e.g. the memory size of USB drives is currently peaking at 32-64 gigabytes). Also worth noting is the prevalence of memory card technology, with card readers now built-in on many laptop computers and computer monitors. The physical and storage size of memory cards, as well as the cost, are comparable to USB drives.

**Key point**

iPods and MP3 players are examples of passive devices. These devices are not simply ‘music players’; they are also storage devices with capacities that typically exceed the USB keys carried by users. In addition to use as portable storage devices, MP3 players typically contain calendaring functionality and can synchronise with desktop software.

**Active mobile and smart devices**

Examples of active mobile and smart devices include:

- digital cameras and video recorders
- smartphones
- laptops
- PDAs.

In the context of this advice, mobile and smart devices with information creation characteristics can be considered ‘active’. Active devices differ from passive devices in that they have the capability to communicate. The devices tend to be personal and they provide information anytime and anywhere. Records can be created, processed, transferred, stored, disseminated, shared, used, and disposed of in and by active mobile and smart devices.
Appendix C: Risks to public records resulting from use of mobile and smart devices

While mobile and smart devices offer a number of benefits through their versatility, they are subject to the same records management obligations as other more established technologies such as desktop computers. However, their mobility means they are exposed to another set of risks and records management challenges that differ from more established technologies.

Lack of access to public records stored on mobile devices has the potential to pose significant recordkeeping risks to government. These risks include:

- lack of capture of public records, resulting in inadequate or incomplete business records
- potential for unlawful disposal of public records
- loss of public records if an employee leaves the public authority and has not previously captured the information into a recordkeeping system (as outlined in section 4.2).

In addition, if public authorities wish to access employees’ personal BYOD devices, there is also potential for privacy and other legal issues (see section 3.4). To assist in overcoming some of the recordkeeping challenges associated with mobile devices, public authorities should focus on ensuring recordkeeping obligations are documented and communicated with employees. Section 4 of this guideline provides an overview of a number of strategies and solutions to manage the recordkeeping implications of mobile devices.

Risks specific to public records resulting from use of mobile and smart devices can be grouped broadly into the following two categories:

<table>
<thead>
<tr>
<th>Data theft / loss</th>
<th>Security compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and smart device loss or theft[^33]</td>
<td>Malware infection of device</td>
</tr>
<tr>
<td>Data loss or theft (e.g. accidental or deliberate if the device fails)</td>
<td>Unauthorised access to data previously stored on the mobile and smart device</td>
</tr>
<tr>
<td>Mobile and smart device infection which may enable remote data theft</td>
<td>Loss of sensitive information from mobile and smart devices due to lack of data classification</td>
</tr>
<tr>
<td>Mobile and smart device data storage may be used for data theft from corporate facilities[^34]</td>
<td>Mobile or smart device may be used as a vector for malware infection of corporate network</td>
</tr>
<tr>
<td>Mobile network may be used for data extraction</td>
<td>Mobile or smart device may be used as a network snooping or attach tool</td>
</tr>
<tr>
<td>Mobile and smart device loss or theft may expose credentials</td>
<td>Introduction of unwanted software onto organisational networks</td>
</tr>
<tr>
<td>Imprecise catalogue of information stored on a lost mobile and smart device</td>
<td>Inability to control, manage, track and monitor mobile and smart devices and information copied onto devices</td>
</tr>
<tr>
<td>Data transfer to a privately owned device or to personal email accounts (or similar)</td>
<td>Unauthorised exposure to sensitive material due to inadequate disposal of devices</td>
</tr>
</tbody>
</table>

[^32]: Although this list is not exhaustive, it provides an overview of the general risks posed to public records resulting from the use of mobile and smart devices.
[^33]: In a high profile Australian example from 2011, a Defence Department contractor left a USB flash drive in the seat pocket of a commercial aircraft. The unencrypted device was handed to a radio announcer. ‘Defence investigates lost and found memory stick’, www.itnews.com.au/News/251084.defence-investigates-lost-and-found-memory-stick.aspx
[^34]: How 250,000 US embassy cables were leaked, www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked
Appendix D: Decision matrix for identifying public records stored within mobile and smart devices

Management of public records created and stored on mobile and smart devices – as well as management of the devices themselves – can be more difficult than managing information held on traditional platforms such as desktop computers and corporate servers. By the very nature of mobile devices, a higher degree of user intervention is likely to be required to ensure records are captured, since they may reside outside of a recordkeeping system’s direct control.

In addition, it is important to consider that ‘mobile data’ consists of many different types of content, all needing to be managed. For example, a mobile device can send, receive or generate email, Webmail, files, SMS/MMS messages, social media content, audio recordings, photographs, video recordings, geolocation information and other types of data. The diversity of formats creates challenges around the identification, creation and capture of public records which may be reside on mobile and smart devices, into recordkeeping systems.

For more information on defining public records, refer to What is a Public Record35.

The following decision matrix (Figure 3) is provided to assist in determining whether information contained within mobile and smart devices could be identified as a public record.

Figure 3: Decision matrix to identify whether mobile and smart devices contain public records

- **Is the information purely personal?**
  - Yes: Not a public record. Does not need to be maintained
  - No: **Is the information mainly ephemeral or facilitative?**
    - Yes: Remove from the mobile and smart device when no longer needed for business purposes
    - No: **Does the information provide evidence of outcomes or decisions made?**
      - Yes: Ensure a record of the information is created and captured in the public authority’s recordkeeping system
      - No: Retain the record for the required period as outlined in an approved Retention and Disposal Schedule

**Notes**

- Information that is purely personal
  - e.g. resume or email asking colleague for lunch
- Business related information
  - e.g. email relating to public authority work activities
- Ephemeral or facilitative information
  - e.g. information or research used to prepare other records
- Evidence of business outcomes or decisions made
  - e.g. information documenting business activity including contracts, project plans, emails giving direction
- Retention of records
  - e.g. retention periods are outlined in sector or agency specific retention and disposal schedules

Appendix E: Guide to storage capacities for mobile and smart devices and related recordkeeping implications

Many mobile and smart devices contain internal memory chips with large storage capacities or provision for an external memory card. The below table provides a guide to how much information can be stored on a mobile and smart device:

<table>
<thead>
<tr>
<th>Document type</th>
<th>Average (per 10 megabytes)</th>
<th>Average (per 100 megabytes)</th>
<th>Average (per gigabyte)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Word files</td>
<td>647</td>
<td>6,478</td>
<td>64,782</td>
</tr>
<tr>
<td>Email files</td>
<td>1,000</td>
<td>10,000</td>
<td>100,099</td>
</tr>
<tr>
<td>Microsoft Excel files</td>
<td>1,657</td>
<td>16,579</td>
<td>165,791</td>
</tr>
<tr>
<td>Microsoft PowerPoint files</td>
<td>175</td>
<td>1,755</td>
<td>17,552</td>
</tr>
<tr>
<td>Text files</td>
<td>6,779</td>
<td>67,796</td>
<td>677,963</td>
</tr>
<tr>
<td>Image files</td>
<td>154</td>
<td>1,547</td>
<td>15,477</td>
</tr>
</tbody>
</table>

For ease of reference:

- 1024 kilobytes = 1 megabyte
- 1024 megabytes = 1 gigabyte
- 1024 gigabytes = 1 terabyte.

For example

An Osterman Research survey conducted in January 2011 found that 4.6% of corporate data was stored just on users’ smartphones. While 4.6% may not sound like an enormous proportion of data, an organisation with a total of just five terabytes of data under management will have 236 gigabytes of data on smartphones.37

The following table provides an example of the storage capacities and approximate costs of various mobile and smart devices:

<table>
<thead>
<tr>
<th>Mobile and smart device type</th>
<th>Amount of data capable of holding</th>
<th>Cost guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB flash drive</td>
<td>Range from 1GB to 256GB</td>
<td>$15 - $20 for a 16GB device</td>
</tr>
<tr>
<td>External hard drive</td>
<td>1 terabyte or more (1000GB)</td>
<td>$90</td>
</tr>
<tr>
<td>Laptop computers</td>
<td>Hard drives range from 250GB to 1 terabyte</td>
<td>$500 - $2000</td>
</tr>
<tr>
<td>Smartphones and PDAs</td>
<td>Up to 64GB</td>
<td>$600 - $800</td>
</tr>
</tbody>
</table>

38 Information provided in the table is a guide only, based on research as at January 2013.
Most mobile or smart devices can be used as a USB mass storage device by simply plugging it into a PC through a USB connection. There is an inherent recordkeeping risk associated with allowing USB mass storage application as significant quantities of public records may be transferred to/from a mobile or smart device with ease. Recordkeeping risks include:

- mobile and smart devices capable of copying and storing large amounts of data without being detected
- low levels of encryption usage when transferring information across potentially unsecured networks
- public authorities may not employ adequate controls for the management of public records through use of mobile and smart devices, and some may rely only on written policies, and
- the communication of policies and procedures is often passive (e.g. posting them on intranets) rather than active (e.g. staff training or management oversight).

Mobile and smart devices (including external hard drives and USB keys) should not be used as data storage repositories for public authority records in place of a formal backup regime. Users should be made aware that informal backup practices are inadequate, and carry the risk of accidental or deliberate loss of public records.

As outlined in section 4.2, public authorities should ensure that information identified as a public record that is contained on a mobile and smart device is transferred and captured into a public authority’s recordkeeping system as soon as practically possible. Appropriate capture strategies will help ensure identified public records are retained and disposed of appropriately, in accordance with an approved Retention and Disposal Schedule.

**Key point**

Regardless of medium, public records take on the retention value of the business transactions which they document, described under a Retention and Disposal Schedule approved by the State Archivist. For example, text messages captured as public records should be retained for the same length of time as other public records documenting the business activity for which purpose the text message was created.

An added complexity of storing data within mobile and smart devices is that rather than information being stored on the internal memory of the device, users (especially if using personal devices under a BYOD arrangement) may use cloud-based services for storing information. Use of cloud computing arrangements raises a number of recordkeeping related issues, particularly in relation to data security and information privacy. Refer to the Queensland State Archives Public Records Brief *Managing the recordkeeping risks associated with cloud computing*[^39] for further information.

**Key point**

Implications of cloud storage for information held on mobile and smart devices and associated recordkeeping and privacy requirements should be considered in mobile and smart device policy and procedures. For example, a feature introduced in Apple’s iOS 5 allowed users to sync and store all of their devices’ data in Apple’s iCloud. Other devices may adopt similar functionality through use of services such as Dropbox.