Text messages

1 Text messages are considered records

If an organisation uses text messaging or any other instantaneous, non-sequential electronic communication mechanism to conduct business, these communications are considered records under the *Public Records Act 2005*. As such, they must be managed accordingly.

2 Core guidance on text messaging

Organisations constantly balance the concerns of providing practical guidance with the needs of employees to use the best electronic messaging systems and devices available to conduct business. Many text messages will be facilitative, transitory, or of short-term value. Simply preventing people using electronic messaging to conduct official business is disproportionate, hard to enforce, and does not acknowledge the various ways employees communicate.

An organisation is best able to evaluate what solutions will suit its needs when it has established:

- the messaging technologies being used
- the proportion of staff using those messaging technologies and how often
- the kind of content that is commonly included in text messages
- the overall risk profile of the text message
- how staff currently handle text messages
- who owns the devices handling the text messages
- the privacy and security risks.

An organisation should consider adopting a mixture of in-house and outsourced technical or "low-tech" procedural solutions to records management, and tailoring those solutions to fit individual needs. Consult with information technology and telecommunications staff and providers to determine which approach best suits an organisation's needs.

3 Technical and compliance issues in managing text messages

An organisation may face **technical issues** when managing text messages. These issues include:

- capability of electronic messaging systems and devices to create a record and metadata
- capture of complete information and records, including usable and sufficient metadata
- verification of user identity
- exposure to viruses and spyware
- lack of a string of text messages that help keep the message in context
- use of non-government software and hardware
- incompatibility of different electronic messaging programs
- digital preservation of information and records that have long-term value.

An organisation must also be aware of **compliance issues** when managing text messages. These issues include:

- mandatory requirements under the *Public Records Act 2005*
- obligations and considerations under the *Privacy Act 1993*
- official information requests and evidence discovery
- accessibility requirements under the *Electronic Transactions Act 2002*
- security considerations.

4 Procedural and technical approaches to managing text messages

The two approaches outlined below offer organisations different yet complementary means of dealing with issues related to managing text messages.

- **Procedural approach**: focuses on ensuring that adequate information and records are created through non-technical (sometimes manual) methods.
- **Technical approach**: focuses on identifying products or service providers that can create adequate information and records from software and technologies that produce text messaging.

4.1 Procedural approaches to managing text messages

A procedural "low-tech" approach to identifying, managing and capturing text messages can include developing policies and procedures, introducing reviews, and training staff.

- **Develop policies and procedures:** addresses some of the management issues noted. One example is how to identify text messages that are *not* facilitative, that are transitory, or that have short-term value, and knowing what to do with these messages.
- **Introduce regular reviews:** ensures policies and processes are kept up to date with changes in technology.
- **Train staff:** ensures staff are trained in simple and practical methods of capturing text messages in official information and records systems. One example is making a file note of the content.

4.2 Technical approaches to managing text messages

Technical solutions available for the management of text messages can include installing new software and technologies, configuring text messaging technologies, and using third-party services.

- **Install mobile device management software:** integrates with official networks and systems to centrally configure, manage and secure applicable text message-capable devices.
- **Use virtualisation technologies:** lets users work in virtual environments through virtualisation or "thin client" solutions.
- **Configure text messaging technologies:** allows for easy and automated capture of electronic messages and metadata.
- **Use a system that allows for export of messages:** ensures that text messages, including metadata, can be exported from the system in which they were originally created.
- **Use third-party services:** captures messages, such as a service that captures all email, chat and text messages created through organisational systems.

4.3 Factors to consider in selecting technical solutions

Nature of solution
Is the solution built into the messaging product, or is it an add-on?
If the solution considered is not in-house (that is, provided by an external service provider), what guarantees about long-term access can the service provider offer?
What format or formats can the message be generated in (or converted into)?
Can the solution interface with existing information and records management systems? If so, does that interface (method or programs) have any restrictions?
Capture method
Does the capture of the text message occur automatically, or does it have to be activated manually?
Does the capture have rules? If so, and the capture is automatic, how flexible are these rules??
Can the capture mechanism be tailored to capture conversational threads?
Can users bypass the capture?
Metadata
What level of metadata can the solution capture?
How customisable is the metadata set?
How automated is the metadata collection?
How secure (tamper-proof) is the metadata set?
Does the solution allow for both manual entry of metadata and automated capture of some elements?
Security and legal compliance
What security measures can be applied to the solution?
What, if any, form of identity verification is offered?
Does the solution comply with relevant legislative and policy requirements? Will the solution enable the organisation to comply with relevant legislative and policy requirements?