MINISTRY OF SOCIAL DEVELOPMENT
Te Manatū Whakahiato Ora

Bowen State Building, Bowen Street, Wellington 6011, PO Box 1556, Wellington 6140 • Telephone: 0-4-916 3300 • Facsimile: 0-4-918 0099

12 NOV 2012

Ms Jessica Fathom
fyi-request-596-fbc00ea4@requests.fyi.org.nz

Dear Ms Fathom

Thank you for your email of 6 October 2012 requesting, under the Official Information Act 1982, the following information:

> *"The policy and procedure around the records management of text messages sent/received on staff work phones. Please also provide any operational documents about how the Ministry ensures all text messages sent/received on staff phones are captured on a document management system – for example, instructions given to staff on record management obligations regarding text messages.*
>
> *Please provide the product description and operational set up of software installed on any staff phones to back up and store text messages to a document management system.*
>
> *Lastly, in the month of September 2012 around how many text messages sent/received on staff phones were stored on the Ministry's central document management system?"*

There are a number of ways in which staff can send or receive text messages:

- 'normal' text messaging to/from Ministry provided mobile phones
- use of the Ministry's staff directory to send a text message from a computer
- use of text message gateways linked to line of business applications, for example for sending text alerts to students.

As you have specifically asked about text messages sent/received on staff work phones, I have not considered policies about automated bulk text messages sent to clients to be in the scope of your request.

The Ministry is guided in its recordkeeping responsibilities by the Public Records Act 2005. The Public Records Act sets the framework for creating and managing information in government. It defines a record as: *"information, whether in its original form or otherwise, including ... a document, a signature, a seal, text, images, sound, speech or data compiled, recorded, or stored... in written form on any material, or on film, negative, tape or any other medium so as to be capable of being reproduced, or by means of any recording device, or process, computer, or other electronic device or process."*

The Ministry's Records Management Policy provides a framework and responsibilities for ensuring that full and accurate records of the Ministry's business activities are created. This policy applies to all Ministry staff, managers and contractors and defines the types of Ministry information that are records. Text messages are not specifically

mentioned in this policy, however consistent with the above definition, it notes that records *'come in a variety of media such as paper, electronic (analogue or digital) and can be documents, letters, emails, digital images, sound recordings, databases or web pages.* Text messages are therefore considered a public record.

The Records Management Policy outlines the responsibilities of managers and staff in respect of record keeping. These include ensuring that staff create adequate, accurate and reliable records and that they are captured in the Ministry's records management and *business* applications. These requirements are expanded on for all Ministry staff in a set of eight records principles. *Principle 2: Capture all records into recordkeeping systems,* states:

- *Records must be routinely captured into organisation wide recordkeeping systems.*
- *Staff will not keep public records in separate, individual file systems, which include hard drives, laptops, and removable storage devices.*

Please find enclosed a copy of the Ministry's current Records Management Policy, including the eight records principles. This policy is available to all staff on the Ministry's intranet.

The principal method of training Ministry employees about records management is an e-learning package available to all staff via the Ministry's intranet. Called 'On the Record' the training addresses much the same ground as the Records Management Policy, namely:

- *Our recordkeeping responsibilities as Ministry employees*
- *Why you need to keep records*
- *How to manage your records effectively*
- *How Records Services can help and support you in your work.*

The section on 'What is a Record' specifically notes that mobile device messages and texts may be records and therefore need to be managed in the same manner as other records. However, text messages are generally used for business messages of short-term value and therefore there would be no requirement to save these messages into the document management system.

There are no other operational documents instructing staff on records management obligations specifically regarding text messages. I have however enclosed for your reference relevant extracts of the recordkeeping intranet pages that contain information relevant to this type of record.

There is no software installed on staff mobile phones to back up and store text messages to a document management system. Incoming text messages are not automatically stored and can only be saved into the Ministry's central document management system (EDRMS) by first converting the text to email and then manually saving this as a document into the document management system. Therefore there is no way to search for documents in EDRMS to identify which originated as a text message.

The Ministry monitors the usage of staff mobile phones by recording the occurrence of all calls from mobile devices (including text messages) capturing the phone number from, phone number to, date and time, into the Risk and Assurance Forensic Tool (RAFT) system. However this does not include the text message content.

I am unable to respond to your request for details of the software installed on staff phones to back up and store text messages, and how many text messages sent and received on staff phones were stored on the Ministry's central document management system in the month of September 2012 under section 18(e) of the Official Information Act as the information does not exist or cannot be found.

I hope you find this information helpful. You have the right to seek an investigation and review of my response by the Ombudsman, whose address for contact purposes is:

The Ombudsman
Office of the Ombudsman
PO Box 10-152
WELLINGTON 6143

Yours sincerely

David Shanks
Deputy Chief Executive Corporate and Governance

MSD Records Management Policy

The MSD Records Management Policy provides a framework and responsibilities for ensuring that full and accurate records of MSD's business activities are created. The current version of the policy was approved by the Leadership Team on September 6th, 2011.

On this Page:

Introduction

Purpose

The purpose of this policy is to provide a framework and assign responsibilities for ensuring that full and accurate records of the business activities of the Ministry of Social Development (MSD) are created. It aims to ensure that these records are managed and maintained for as long as they are required to support business functions and accountabilities, until their disposal in accordance with the appropriate authorised retention and disposal schedule.

Scope

This policy applies to ALL Ministry staff nationwide, that is Corporate, Policy and Service Delivery business groups regardless of their location throughout New Zealand and includes:

- Regions, Regional Offices, and National Office
- All MSD staff, whether permanent, temporary, or contractors
- All contracted service providers, where they are required to create and maintain records of their activities on behalf of MSD
- All inter-agency initiatives, where MSD is the lead agency and/or where it is agreed that MSD owns or is responsible for the resulting records.

This policy applies to all business activities performed by, or on behalf of, the Ministry. This includes all written and spoken transactions, whether paper or electronic.

Equally, it covers all records of these activities, regardless of the media / format in which they are created and captured.

Policy

Overview

The Ministry relies on its records to operate efficiently and account for its actions. The organisation's records are our corporate memory, forming a core knowledge base preserving and providing evidence of advice, actions and decisions; they represent a vital organisational asset to support our daily functions and operations.

Records support policy formation and managerial decision-making, protect the interests of the Ministry and protect the rights of staff and members of the public who have dealings with the agency. Records support consistency, continuity, efficiency and productivity and support the Ministry to deliver its services in consistent and equitable ways.

This policy is required as part of the record keeping framework established by the Public Records Act 2005 and is based on the Archives NZ best practice guide "A Guide to Developing a Recordkeeping Policy". It defines a structure for the Ministry to ensure adequate records are created and maintained. It ensures records are managed and controlled effectively and add best value, commensurate with legal, operational and information needs.

Statement

All of the Ministry's records are Public Records under the Public Records Act 2005 and must be kept in accordance with statutory and industry standards or guidelines.

The Ministry is committed to achieving government aims as stated in the Public Records Act 2005. It will ensure support for all staff to achieve the outcomes of the Ministry and delivery of services to the public and to government. The Ministry affirms that the promotion and practice of good recordkeeping is a key strategic focus for meeting these outcomes.

This requires the creation, management and authorised disposal of full and accurate records that support the day-to-day functions and business activities of the Ministry. These records provide evidence of these functions and activities and form part of the public record. Through its commitment to good recordkeeping practice, the Ministry acknowledges its accountability to government, to its clients, and to the community.

Records policies, standards and guides provide further interpretation and rules. These should be read in conjunction with the Records Management Policy.

Definition

The Public Records Act defines a record as: "information, whether in its original form or otherwise, including ... a document, a signature, a seal, text, images, sound, speech or data compiled, recorded, or stored... in written form on any material, or on film, negative, tape or any other medium so as to be capable of being reproduced, or by means of any recording device, or process, computer, or other electronic device or process."

Broadly speaking, a record is any **documentation** or **evidence** of activity and/or decision making. They may be the means by which a transaction occurs, such as a contract or letter seeking or receiving information, or they may be created to reflect a transaction, such as minutes taken at a meeting or an electronic payment of an invoice. The information that contributed to a transaction or its outcome can also constitute part of the record.

In summary, records:

1. Provide **documentation**, or **evidence**, of activities
2. Include both **original** sources of information and **copies** of information
3. Come in a **variety of media** / formats such as paper, electronic (analogue or digital), and can be documents, letters, emails, digital images, sound recordings, databases, or web pages.

Summary of requirements

A summary of the key principles and requirements of the Public Records Act and standards are as follows:

1. **Create and maintain full and accurate records.**
2. **Capture all records into recordkeeping systems.**
3. **Make authoritative and reliable records of business.**
4. **Ensure records are accessible, usable, retrievable, and preserved.**
5. **Ensure records are complete and comprehensive.**
6. **Records are secure, protected and stored appropriately.**
7. **Retention and disposal of records is authorised.**
8. **Staff are trained in recordkeeping processes and systems.**

A more detailed outline of these principles and requirements is attached as **Appendix A**.

Ministry responsibilities

DCE Corporate and Governance

The Chief Executive (CE) is ultimately responsible for ensuring that the Ministry meets its statutory obligations. On the CE's behalf, the **DCE, Corporate and Governance** will provide oversight of record keeping processes and practices across the Ministry. This involves:

- Ensuring compliance with the Public Records Act and mandatory standards issued under the Act.
- Gaining approval for the recordkeeping policy.
- Assigning responsibilities for recordkeeping.
- Supporting recordkeeping in the Ministry.
- Ensuring that corporate policies support the creation and maintenance of full and accurate records of the Ministry's functions and activities.
- Ensuring that the Ministry's recordkeeping policies and procedures will meet best practice guidelines and stand up to external scrutiny.
- Ensuring that no illegal records disposal takes place.

Security, Integrity and Business Continuity Advisory Committee (SIBC)

The **Security, Integrity and Business Continuity Advisory Committee** (SIBC) provide oversight of record keeping practices as a sub committee of the Leadership Team. This involves:

- Providing support, direction and guidance.
- Overseeing specific MSD security, integrity and business continuity work programme, such as internal fraud, records management, code of conduct and IT security policies.
- Maintaining and developing standards and enhancement programmes.

- Making recommendations to MSD's Leadership Team on security, integrity and business continuity initiatives.

Chief Information Officer

The **Chief Information Officer** is responsible for ensuring that:

- The Ministry has an IT architecture and infrastructure that supports the aims and implementation of this policy.
- IT solutions / databases in design, development, implementation, and decommissioning of business and information systems complies with recordkeeping requirements.
- Systems / databases are not disposing of records, unless specifically authorized to do so by the General Manager, Information Services.

General Manager, Information Services

The **General Manager, Information Services** is responsible for ensuring:

- Ministry recordkeeping standards and guides support the aims of this policy and are communicated throughout the organisation.
- Provision of high quality advice for senior managers and business groups on the recordkeeping policies, processes and standards issued under the Public Records Act (PRA) 2005.
- Record keeping, and where appropriate business systems, are designed and managed in accordance with the PRA and mandatory standards.
- Regular and periodic reporting to Archives NZ on the Ministry's record keeping responsibilities.
- Ministry recordkeeping practices and systems are monitored and audited for compliance.
- Retention and disposal of records is authorised and no illegal records disposal takes place.
- storage of records held onsite and transferred to offsite facilities complies with the Storage Standard.
- Staff are sufficiently trained and supported in the appropriate use of the Ministry's recordkeeping systems.
- Policies, standards and procedures are regularly reviewed to ensure that they are relevant, useful, and meet the Ministry's needs.

Deputy Chief Executives (DCE)

DCE's are responsible for ensuring that their managers and staff adhere to the record keeping policies, standards and practice guides. This involves:

- Ensuring that record keeping practices and systems meet statutory requirements and any other Ministry standards or guidelines.
- Nominating a staff member from their business group, to be a member of a whole of Ministry Records Network group, chaired by the Manager, Records.
- Embedding a culture of robust record keeping amongst their staff.
- Ensuring staff, contractors and consultants create and capture adequate, accurate, and reliable records on behalf of the Ministry.
- Ensuring staff capture records into the Ministry's records management and business applications.
- Ensuring staff describe records in a meaningfully way so that named it can be found and reused again.
- Ensuring staff handle records with care so as not to damage or change them, or prevent unauthorised access to records.
- Ensuring staff store records that are no longer actively used in approved offsite facilities.
- Ensuring staff are deleting and destroying records in accordance with the recordkeeping standards and guides.
- Ensuring staff are inducted and adequately trained in recordkeeping policies, processes and systems.

Regulatory framework

Legislation and codes

Relevant legislation with which this policy complies includes, but is not limited to:

- Public Records Act 2005
- Official Information Act 1982
- Privacy Act 1993
- Employment Relations Act 2000
- Electronic Transactions Act 2002
- Adoption Acts (1955, 1985, 1997)

- Social Security Act 1964
- Children, Young Persons, and their Families Act 1989
- Public Finance Act 1989.

This policy also complies with the following Standards and Codes:

- Public Service Code of Conduct
- International Standard on Records Management, ISO 15489
- Archives New Zealand *Continuum Resource Kit* (contains standards and best practice advice in the form of guides and fact sheets)
- MSD Information Management Principles 2003.

Relationship with other documents

This policy also supports the Ministry's Information Management Principles.

MSD Information Management Principles

Standards and guides in support of this policy may include (without limitation) all or any of the following matters:

- Records Creation and Maintenance
- Classification Schemes
- Metadata
- Digitisation
- Security and Access
- Retention and Disposal.

Monitoring and review

This policy will be regularly monitored and reviewed to ensure that it remains relevant to the organisation's business aims and requirements. Staff compliance with the policy and associated procedures will be monitored on an ongoing basis through staff self-assessment and by group managers, and by the Records Manager(s).

The next date for policy review is July 2012. The review will be conducted by the Records Manager(s).

Appendix A: Record principles and requirements

Principle 1	**Create and maintain full and accurate records** All staff will create and maintain full and accurate records to account fully and transparently for all actions and decisions, in particular to: • Provide credible and authoritative evidence • Protect legal and other rights of clients, staff or those affected by those actions • Facilitate audit or examination.
Principle 2	**Capture all records into recordkeeping systems** • Records must be routinely captured into organisation wide recordkeeping systems. • Staff will not keep public records in separate, individual file systems, which include hard drives, laptops, and removable storage devices.
Principle 3	**Make authoritative and reliable records of business** • Systems will accurately document details of a record's creation, receipt and transmission • Records' contextual and structural integrity must be maintained overtime • Records are reliable, tamper-proof, and where any changes occur these are recorded in audit trails or logs
Principle 4	**Ensure records are accessible, usable, retrievable, and preserved** • Records and the information within systems can be efficiently retrieved by those with a legitimate right of access, for as long as the records are retained. • Records will be held in robust, durable formats which remain readable for as long as they are required.

- Records of ongoing value will be identified and be accessible over time.
- Business critical / vital records will be identified and accessible when needed

Principle 5

Ensure records are complete and comprehensive

- Records must record the content and contextual information necessary to document a business activity, decision, or key process.
- Records must be made of all areas of business activity and at all relevant points within a workflow or business process.

Principle 6

Records are secure, protected and stored appropriately

- Records will be protected from misuse, unauthorised or inadvertent alteration, loss, or erasure.
- Access and disclosure will be properly controlled; and audit trails will track all use and changes.
- Records are secure against theft, vandalism, or inadvertent release.
- Records that are no longer actively used are stored in offsite storage facilities that enable access and ensure preservation for as long as they are required.
- Records are stored in environmental conditions, outlined in the Archives NZ Storage Standard, which will ensure they are preserved for as long as they are required.

Principle 7

Retention and disposal of records is authorised

- Records, in any format, must be disposed of lawfully, according to disposal schedules approved by Archives New Zealand.
- Deletion or transfer of records occurs regularly, is monitored and reviewed.
- Methods used to dispose of records must comply with any privacy and security requirements.
- Everything necessary and practical must be done to ensure that the destruction of records is complete.
- Records of archival value that are 25 years or older will be transferred to Archives NZ.
- There are consistent and documented retention and disposal procedures which include provision for permanent preservation of archival records.

Principle 8

Staff are trained in recordkeeping

- All staff will be made aware of their recordkeeping responsibilities through generic and specific training programmes and guidance.

Original policy in Word format - held in EDRMS

Content owner: Information Services **Last updated:** 21 July 2012

What is a record?

In the course of a working day, people create, receive, or use records, data, and information of all types. But what is a record and what do you need to do with them?

On this Page:

The Public Records Act

The Public Records Act 2005 makes government organisations responsible for creating and maintaining full and accurate records of their activities. This includes activities undertaken on their behalf by independent contractors.

These records have special significance because they support governments' accountability and provide information about New Zealand's government, society and citizens. Over time, they provide a corporate memory for the organisations that created and used them, and a collective memory for the New Zealand government as a whole.

Public Records Act (PDF 31.59KB)

Staff responsibilities under the Public Records Act

All Ministry staff are required to keep full and accurate records. This includes staff from all Corporate, Policy and Service Delivery business groups regardless of their location throughout New Zealand and regardless of whether they are permanent or temporary staff, contractors or contracted service providers.

Broad definition of a record

Broadly speaking, a record is any documentation or evidence of activity, for example:

- a contract or letter seeking or receiving information
- minutes taken at a meeting
- an electronic payment of an invoice
- service line records

The information that contributed to the creation of such a document or its outcome could also be part of the record.

The Public Records Act defines a record as: "information, whether in its original form or otherwise, including ... a document, a signature, a seal, text, images, sound, speech or data compiled, recorded, or stored... in written form on any material, or on film, negative, tape or any other medium so as to be capable of being reproduced, or by means of any recording device, or process, computer, or other electronic device or process."

So, a record could take almost any form.

In summary, records:

1. Provide documentation, or evidence, of activities;
2. Include both original sources of information and copies of information; and
3. Come in a variety of media / formats.

Creating and maintaining records

Full and accurate records must be:

- **Comprehensive**: they must document all the activities your organisation undertakes
- **Accurate**: they must correctly reflect what was communicated, decided or done
- **Complete**: they must also contain information needed to understand the record (e.g. date, author, links to other records)
- **Created, captured and managed within a records management system**: they must be part of a the official MSD filing system that accommodates paper and electronic records. Staff members must not keep MSD records, for any longer than necessary, in personal folders or files such as personal email folders.

Keeping records

We must keep information that has been created or received in the course of MSD's affairs, which documents or supports our fiscal, legal and business transactions or functions.

Records Managers are the only people authorised to approve records for disposal or destruction.

The table below gives some examples of the types of records which must be kept along with examples of records which can be destroyed at some stage.

Must be kept	Not required
Decision papers	Circulated information received for information only, e.g. listservs, internal circulars, bulletins
Policy briefings and recommendations	Trivial work-related material, such as reminder notes or room bookings
Email and other correspondence	Copies of documents or publications kept for reference purposes, as long as the original records are in the official MSD recordkeeping system
Reports	Preliminary drafts and working papers not significant to decisions made
Publications, including those received from external sources and used for research or official business	Advertising material received where no action was taken
Memoranda	Private or personal correspondence, created or received at work but not affecting official duties and decisions
Minutes of Meetings	
Supporting materials, such as: substantive drafts, annotated documents, reports	
Data in financial management, case management, or human resources information systems	

MSD information principles

Your role in managing information

Content owner: Information Services **Last updated:** 21 July 2012

What emails do I need to keep as a record?

A helpful guide to what emails need to be kept as records.

On this Page:

Emails that need to be kept as a record

To maintain complete, accurate and reliable evidence of business transactions it is essential to manage all correspondence, including email as records.

Think of an email as any other business record – it needs to be kept if it provides documentation or evidence of a business activity.
For example:

- It contains information to help you carry out your work
- It approves or authorises an action
- It contains information that has been used to make a business decision
- It provides evidence of a business process
- It will help others to trace how a decision, policy etc has developed over time

Please bear in mind that sometimes the attachment within an email contains the information that needs to be retained as the business record.

Emails that do not need to be kept as a record

- Personal emails
- Trivial work-related material (such as meeting arrangements)
- Casual discussion with colleagues that do not influence business decisions
- Emails where the attachments may infringe copyright (such as journal articles)

Contact Records Services

Please contact Records Services if you have any queries or questions regarding what emails need to be kept as a record:

Contact Records Services

Content owner: Information Services **Last updated:** 21 July 2012