

Collection and storage of staff personal mobile phone numbers for use in agency generated SMS notifications during emergencies and other business disruptions affecting the Office of the Commonwealth Ombudsman

PRELIMINARY

February 2020

Privacy Impact Assessment Report – Contents

1. Threshold assessment	2
2. Plan the PIA	2
3. Describe the project	2
4. Identify and consult with stakeholders	3
5. Map information flows	4
6. Privacy impact analysis and compliance check	9
7. Privacy management - addressing risks	16
8. Recommendations	17
9. Sign off.....	17

PRIVACY IMPACT ASSESSMENT

Collection and storage of staff personal mobile phone numbers for use in agency generated SMS notifications during emergencies and other business disruptions affecting the Office of the Commonwealth Ombudsman

1. Threshold Assessment

- a) Will any personal information be collected? If yes, record a brief description of the personal information that will be collected, used or disclosed (such as name, address, date of birth, health information etc.).

Office of the Commonwealth Ombudsman (the Office) staff names and personal mobile phone numbers.
--

2. Plan the PIA

General Description

Name of Program: Collection of staff personal mobile telephone contact information
Date:
Name of Section/Branch: Governance, Corporate Branch
PIA Drafter: Melanie Lyon
Email: melanie.lyon@ombudsman.gov.au Phone: (08) 7088 0616
Program Manager: Rodney Lee Walsh
Email: rodney.walsh@ombudsman.gov.au

Definition – Project: For the purpose of this document, the term project is intended to cover the full range of activities and initiatives that may have privacy implications including:

- policy proposals
- new or amended legislation, programs, activities, systems or databases
- new methods or procedures for service delivery or information handling
- changes to how information is stored

3. Describe the Project

In the event of an emergency affecting any office location, the Office is committed to implementing a clear and immediate communication strategy to ensure staff safety as a priority. This communication is especially important during an evacuation and / or event that prevents physical access to an office location.

The Office is therefore proposing to implement a process by which staff may volunteer to provide their personal mobile numbers so that they can be contacted during an emergency and / or disruptive event via the Office's existing SMS service, Optus SMS Suite – powered by Redcoal.

In addition to alerting staff about an emergency, the SMS notification service will also be used to update staff during the activation of a Business Continuity Plan or other disruptions that may prevent them from performing business as usual, for example: ongoing network or power outages.

The Office will also ensure that staff, who wish to receive notifications during an emergency and / or disruptive event, but do not wish to have their information stored in the SMS notification service, will have the option to provide their personal mobile numbers to nominated custodians.

4. Identify and consult with stakeholders

- SLG
- COO / Privacy Champion
- ICT
- Legal Team / Privacy Officer
- Information and the opportunity to make enquiries will be provided to staff prior to implementation of the project

Key privacy elements

- Principle 3 – Collection of solicited personal information
- Principle 5 – Notification of the collection of personal information
- Principle 6 – Use or disclosure of personal information
- Principle 10 – Quality of personal information
- Principle 11 – Security of personal information
- Principle 13 – Correction of personal information

3. Map Information Flows

VERIFICATION

SMS notification system

No formal identity verification is required – only personal mobile phone numbers and names will be collected from individual staff members and subsequently maintained by nominated information custodians responsible for maintaining the SMS notification system.

These information custodians may include:

- Members of the Governance and Communication team and / or
- Members of the ICT team

Persons who could have secondary access to this information may include:

- Employees of the external SMS notification system

Further information regarding the role of information custodians in collecting this information is provided in the following section – Collection.

Where relevant staff are no longer employed by the Office, there will be arrangements to delete their names and mobile telephone numbers from stored records.

Third parties shall not provide or be requested to provide another staff member's personal contact details to an information custodian (or other staff member), except in the circumstances permitted under Australian Privacy Principle 6 and / or other provisions of the *Privacy Act 1988*.

Other storage media – *guidance only*

Staff will have the option to provide their personal mobile numbers directly to other nominated information custodians to enable phone contact in the event of an emergency or disruptive event.

These information custodians will be individually responsible for following the relevant Australian Privacy Principles.

The Governance and Communication team will not be responsible for coordinating the collection, storage or maintenance of this information or any privacy breaches occurring in relation to this information.

COLLECTION

What

- Staff names and personal mobile phone numbers, as personally volunteered by staff
- Staff will be provided with the option to not provide this information.
- Personnel records will not be accessed or requested by any staff member other than HR
- Sensitive information will not be collected
- Staff include persons employed by the Office under a contract of service

Why

To collect staff personal mobile numbers for the Office to distribute SMS notifications about emergencies and / or business disruptions with the intent of maintaining staff safety and essential functions / activities.

Who

SMS notification system

The collection and maintenance of this information will be undertaken by the Governance and Communication team. ICT may also undertake this work, if required in the circumstances.

Other storage media

An option will be provided for staff to consent for their phone numbers to be stored on their line-manager's and / or office site manager's work mobiles.

The collection of this information will be undertaken by the following information custodians in the first instance:

- Direct line managers
- Office site managers

These information custodians will be nominated by virtue of their substantive positions as line managers and / or office site managers. It is preferable if these custodians are at either EL1 or EL2 level. However, other classifications may be considered at the discretion of the relevant line manager.

These information custodians will be individually responsible for collecting, storing and maintaining this information and following the relevant Australian Privacy Principles and the Office's Privacy Policy.

The Governance and Communication team will not be responsible for coordinating the collection, storage or maintenance of this information or for any privacy breaches occurring in relation to this information.

Responsibilities

Prior to engaging in any information collection, all information custodians will be informed of their responsibilities under the *Privacy Act 1988* and Australian Privacy Principles and be expected to comply with them accordingly.

An allegation of information mishandling made against any information custodian must be submitted to the Office's Privacy Contact Officer and / or the affected person's SAO and managed per the Office's Privacy Guidelines.

Pending, and for the duration of any investigation of the allegation, the information custodian must not continue performing this role. The information custodian's SAO will be responsible for applying and monitoring this restriction and ensure that the information custodian removes all records of the alleging party's personal contact details from any medium in which they have stored that information.

How

SMS notification system

The Governance and Communication team and / or ICT team will be responsible for entering and storing staff mobile phone numbers and names in the [Optus SMS Suite](#) – powered by [Redcoal](#).

As the existing SMS notification service does not currently support an opt-in function and is not generally accessible to all staff, the required data will be manually collected by nominated information custodians. The following collection methods have been proposed:

- **Hard copy** – staff may be asked to fill out a form / list
- **Email** – staff may be asked or request to provide this information via email

Any electronic documentation containing this information, including scanned hardcopy lists, consent forms and emails, must be saved into a secure location in Objective. Any scanned hardcopy document containing this information, must be disposed of in a secure bin.

Other storage media – guidance only

Line manager and / or office site manager work mobiles - An option will be provided for staff to consent for their phone numbers to be stored on their line-manager's and / or office site manager's work mobiles. These information custodians will be individually responsible for collecting, storing and maintaining this information and following the relevant Australian Privacy Principles and the Office's Privacy Policy.

The Governance and Communication team will not be responsible for coordinating the collection, storage or maintenance of this information or for any privacy breaches occurring in relation to this information.

USE

SMS notification system

The Office is proposing to implement a process by which staff can receive notifications during an emergency and / or disruptive event via the Office's existing SMS service, [Optus SMS Suite](#) – powered by [Redcoal](#).

In the event of an emergency affecting office premises, the Office and/or information custodians will distribute SMS notifications to alert local staff of the event and what steps are being taken to maintain their safety.

In addition to alerting staff about an emergency, the SMS notification service will also be used to advise staff of the activation of a Business Continuity Plan or other disruptions that may prevent them from performing business as usual, for example: ongoing network or power outages.

Ongoing updates will also be provided on the status of an event and what is being done to manage the impact on the Office's critical functions and to return to business as usual.

Other notification methods

- **Line manager and / or office site manager work mobiles**

The Office will also ensure that staff, who wish to receive notifications during an emergency and / or disruptive event, but do not wish to have their information stored in the SMS notification system have the option to consent for their phone numbers to be stored on their line-manager's and / or office site manager's work mobiles. These information custodians will be individually responsible for collecting, storing and maintaining this information, following the relevant Australian Privacy Principles and the Office's Privacy Policy.

The Governance and Communication team will not be responsible for coordinating the collection, storage or maintenance of this information or for any privacy breaches occurring in relation to this information.

- **Consent**

Where required or requested, a consent form will be provided to staff wishing to provide their personal mobile numbers to nominated custodians for the express purpose of receiving notifications and updated regarding an emergency and / or other business disruption.

- **Data linkage / matching**

It is not envisaged that any personal information provided by staff will be linked, matched or cross referenced with any other external or internal data source, other than the Optus SMS notification system.

DISCLOSURE

With the exception of emergency services, the Office has undertaken to ensure that this information will not be disclosed to any further class of internal / external parties not referenced above.

The Office will not disclose this information to overseas recipients.

INFORMATION QUALITY

Collection

Staff will be asked to provide their personal mobile phone numbers directly to those information custodians responsible for collecting this information.

With the exception of an immediate crisis / emergency where an individual's safety is at imminent risk, staff may not provide or be requested to provide another person's mobile number to a third party for the purposes of this project – this includes where a staff member has asked another person to provide these details.

Custodians must ensure to verify the details with the staff member providing it. A data entry form may be developed to assist with this process.

Regular requests for staff to confirm any changes to their mobile phone numbers and / or names will be distributed. Staff will be personally responsible for ensuring that they confirm any changes.

For collection methods, refer to information provided on page 6.

Storage

- **SMS notification system** - Custodians responsible for entering staff names and mobile phone numbers into the SMS notification system (Governance and Communication team and / or ICT team) will only be expected to rely on the veracity of the information provided to them but will be responsible for ensuring to enter that information as provided by the staff member.
- **Objective** - It is recommended that, dependent on staff consent, once the information has been collected from staff via any of the methods described on page 6, it is entered into a central and secure Objective folder that is individually accessible by relevant information custodians. This will provide one source of information and reduce the risk of numbers being incorrectly recorded via multiple forms of transmission ie verbal to email to SMS notification system
- **Line manager and / or office site manager work mobiles** - An option will be provided for staff to consent for their phone numbers to be stored on their line-manager's and / or office site manager's work mobiles. These information custodians will be individually responsible for collecting, storing and maintaining this information and following the relevant Australian Privacy Principles and the Office's Privacy Policy.

The Governance and Communication team will not be responsible for coordinating the collection, storage or maintenance of this information or for any privacy breaches occurring in relation to this information.

Consequences

If the personal mobile number of a staff member is not recorded correctly, the following may occur:

- The staff member will not receive any notifications relating to emergencies and / or business disruptions affecting the Office, which may result in them not avoiding the threats posed by the emergency and / or not being aware of any actions the Office undertakes to return to business as usual.
- A third party not related to the Office could receive notifications, which has the potential for them to take advantage of property vulnerabilities, including access to evacuated buildings with disarmed locks and subsequent access to information / assets etc.
- A staff member's identity could be disclosed via unauthorised access to their personal information.

SECURITY

SMS notification system

- The Optus SMS Suite employs Two Factor Authentication (2FA).
- Further details about the security and privacy safeguards employed by the SMS notification system, refer to the [Redcoal Privacy Policy](#).
- To prevent the unauthorised disclosure of any other person's personal information, staff will not be able to view their information as entered into the active SMS notification system.

The Governance and Communication team will not be responsible for coordinating the collection, storage or maintenance of this information or for any privacy breaches occurring in relation to this information.

Other storage media – guidance only

- **Objective** - For electronic information not stored in SMS notification system, secure folders in Objective are recommended.
- **Line manager and / or office site manager work mobiles** - In the event staff have consented for their phone numbers to be stored on their line manager's and / or office site manager's work mobiles or other alternative media, these information custodians will be individually responsible for following the relevant Australian Privacy Principles and the Office's Privacy Policy. Staff must also be provided with and return a signed confidentiality statement to the custodians.
- **Hard copy** - Where any staff who have provided their phone number do not wish for that information to be stored electronically, a hardcopy format will be stored in a secure location (ie in a locked drawer / cabinet) and only accessible by nominated custodians of that information. However, storage method is not recommended, as this will prevent access to the information in an emergency if a custodian is not present in an office location during an emergency.

RETENTION AND DESTRUCTION

SMS notification system

Staff who have provided their personal phone numbers for use by the SMS notification system for the purposes of being notified of emergencies and other business disruptions will be responsible for advising the relevant information custodians - Governance and Communication team and / or ICT - when they no longer wish to have their personal phone number and name stored in this format.

Staff must also advise these information custodians if and when they will no longer be employed by the Office in any form.

These information custodians responsible for maintaining this information in this format are responsible for ensuring that this information is removed from or de-identified in this source.

The Governance and Communication team and / or ICT team will only be responsible for ensuring this information is removed from the SMS notification system.

Other storage media – guidance only

Line manager and / or office site manager work mobiles - These information custodians will be individually responsible for collecting, storing and maintaining this information and following the relevant Australian Privacy Principles and the Office's Privacy Policy. They will also be responsible for ensuring this information is retained / destroyed following the departure of any staff whose details they have stored in any media for the purpose of notifying them of an emergency or other business disruption.

The Governance and Communication team will not be responsible for the maintenance or destruction of this information.

ACCESS AND CORRECTION

SMS notification system

To prevent the unauthorised disclosure of any other person's personal information, staff will not be able to view their information once it is entered into the active SMS notification system.

If required, workarounds, such as system generated reports, edited screen shots etc will be considered.

Other storage media – guidance only

Similar actions may be relevant in allowing staff to access any other medium used to record staff personal mobile numbers (such as hard copy or electronic lists). Information custodians responsible for maintaining these resources will be responsible for how they manage requests to access this information.

Update requests

Regular requests for staff to update the information stored in either the SMS notification system and / or other mediums used to record staff personal mobile numbers will be circulated by the Governance and Communication team and / or COO.

Governance and Communication team and / or ICT will make amendments to this information in the SMS notification system. Custodians who maintain this information in other formats will be responsible for ensuring it is updated, as required.

Staff may, at any time request amendments to their information stored in either the SMS notification system and / or other formats used to record staff personal mobile numbers.

Staff may also request at any time that their information be removed from these resources. The custodians responsible for maintaining these resources will be required to action such requests at the earliest possible time following the request.

While it is preferable that any of the above requests are made in writing to ensure the veracity of any amendments, staff may choose to submit the request verbally. The custodians responsible for maintaining this information must confirm the changes with the staff member requesting them. A form will be available to assist with this process.

6. Privacy Impact Analysis and Compliance Check

PRIVACY IMPACT ANALYSIS

Personal mobile numbers may be recognised as personal information as defined by the *Privacy Act 1988*.

The agency must therefore take reasonable steps to protect this information.

Collection of staff personal mobile numbers can be considered as coming under the Office's 'corporate functions / activities' as described in p.10 of the *Office's Privacy Policy*.

Personal mobile phone numbers will only be collected directly from the owner of that information. Exceptions may be considered under Australian Privacy Principle 6 and / or the *Privacy Act 1988*.

Except as explicitly identified by a staff member providing their personal details, the type of information collected is not considered 'sensitive'.

Confidential personnel records will not be accessed to retrieve this information.

Where required or requested, a consent form will be provided to staff wishing to provide their personal mobile numbers to nominated custodians for the express purpose of receiving notifications and updated regarding an emergency and / or other business disruption.

Complaints

Staff will be advised to contact the Office's Privacy Contact Officer if they believe that their personal information has been breached, misused or otherwise compromised.

If staff are unhappy with how their complaint is handled, they can make a complaint to the Office of the Australian Information Commissioner. Information about how to do this can be found on OAIC's [website](#).

ENSURING COMPLIANCE

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	<p>Principle 1 – Open and transparent management of personal information</p> <p>The agency must have a clearly expressed and up to date APP privacy policy about the management of personal information by the agency.</p>	<p><i>OCO Privacy Policy –does not contain specific guidance on the collection and storage of staff’s contact information. However, storage of mobile telephone numbers in a secure manner as per staff personnel records would meet applicable requirements.</i></p>	Complies	
2	<p>Principle 2 – Anonymity and pseudonymity</p> <p>Individuals must have the option of not identifying themselves, or of using a pseudonym, note exceptions to this rule apply.</p>	<p><i>Staff names will need to be provided for entry into the SMS notification system. It is therefore not practical to offer this option if a staff member wishes to voluntarily provide their personal mobile number for the purposes of receiving notifications through this medium.</i></p> <p><i>Further discussion as to the practicality of letting staff provide their mobile number with or without a pseudonym for alternative storage methods (ie electronic or hard copy lists) for the specified purposes will be investigated.</i></p>	Complies	
3	<p>Principle 3 – Collection of solicited personal information</p> <p>Limits apply to only collect information where the information is reasonably necessary for or directly related to one or more of the agency’s functions or activities.</p>	<p><i>The collection of this information is considered reasonably necessary for, or directly related to, the Office’s corporate functions and / or activities.</i></p> <p><i>The Office will ensure that staff understand that it is in their interests to consent providing their mobile phone numbers and names to allow the Office and delegated officers to contact them in an emergency and / or other business disruption that may impact on their safety and / or attendance.</i></p> <p><i>In doing so, the Office will ensure that staff are provided with adequate information about why and how their names and personal mobile numbers will be collected, stored and used, as well as who will be responsible for each of these actions.</i></p> <p><i>Staff may not provide another person’s personal mobile number to another person for the purposes of this project – this includes where a staff member has asked another person to provide these details.</i></p>	Complies	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
		<p><i>Exceptions to obtaining a staff member's personal mobile number will be considered in the following circumstances:</i></p> <ul style="list-style-type: none"> - <i>Where there is a high probability of a risk to that staff member's safety; and</i> - <i>It is unreasonable or impractical to collect it directly from the staff member.</i> <p><i>Agency staff handling the personal mobile numbers of other staff will be advised that they:</i></p> <ul style="list-style-type: none"> - <i>Are required to comply with the relevant Australian Privacy Principles</i> - <i>They must not coerce / pressure staff into providing this information</i> - <i>Notify the Agency's Privacy Contact Officer if they believe a privacy breach has occurred.</i> <p><i>Although the type of information to be collected is not sensitive, staff will be given the opportunity to voluntarily provide express consent for their personal mobile number to be collected and used for the specified purposes by completing a written consent form.</i></p>		
5	<p>Principle 5 – Notification of the collection of personal information</p> <p>Inform the person what information you are collecting, the purpose or use of the information and how they may access or complain about the use of the information. Also inform them if the agency is likely to disclose the information to overseas recipients.</p>	<p><i>The Office will provide explanations for collecting staff names and personal mobile numbers for specific use in the event of an emergency and / or other business disruption that may impact on their safety and / or attendance at work.</i></p> <p><i>In doing so, the Office will ensure that staff are provided with adequate information about why and how their names and personal mobile numbers will be collected, stored and used, as well as who will be responsible for each of these actions.</i></p> <p><i>Preliminary notification of the proposed SMS system has been provided to staff via an Office intranet article: An office-wide SMS notification system will be implemented.</i></p> <p><i>The Office will ensure that staff understand that it is in their interests to consent to providing their mobile phone numbers and names for these purposes.</i></p> <p><i>Staff responsible for collecting this information will be advised that they must not coerce / pressure staff into providing this information</i></p>	Complies	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
		<p><i>A consent form outlining the purpose and voluntary nature of this request has been drafted and attached to assessment.</i></p>		
6	<p>Principle 6 – Use or disclosure of personal information</p> <p>Use it for the purpose you collected it for, unless one of the exceptions applies.</p>	<p><i>The Office will only use staff personal mobile numbers to notify them of an emergency affecting office locations and update them on the status of ongoing business disruptions that may impact on their safety and / or attendance.</i></p> <p><i>The Office will ensure that staff are provided with adequate information about why and how their names and personal mobile numbers will be collected, stored and used, as well as who will be responsible for each of these actions.</i></p> <p><i>If applicable, disclosure and use of staff names and mobile numbers to third parties in the absence of consent, may be considered under Privacy Act 1988 Part VIA—Dealing with personal information in emergencies and disasters and / or the following exceptions:</i></p> <p><i>‘...it is needed to address a serious and imminent threat to life or health and it is unreasonable or impracticable to obtain consent...’</i></p> <p><i>‘...it is necessary to locate a missing person...’</i></p> <p><i>Although the type of information to be collected is not sensitive, staff will be given the opportunity to provide express consent for their personal mobile number to be collected and used for the specified purposes by completing a written consent form.</i></p> <p><i>Staff will also be advised of the Office’s complaints process regarding suspected privacy breaches.</i></p>	Complies	
7	<p>Principle 7 – Direct marketing</p> <p>Information not to be disclosed for the purpose of direct marketing unless exceptions apply, e.g., consent.</p>	<p><i>The Office will not disclose or allow staff personal information to be disclosed for the purpose of direct marketing.</i></p>	Complies	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
10	<p>Principle 10 – Quality of personal information.</p> <p>Ensure information is accurate, up to date, complete and relevant prior to using it.</p>	<p><i>The Office, will request staff to provide their personal mobile phone numbers directly to those custodians responsible for collecting this information.</i></p> <p><i>Staff may not provide another person’s personal mobile number for the purposes of this project – this includes where a staff member has asked another person to provide these details.</i></p> <p><i>Exceptions to obtaining a staff member’s personal mobile number will be considered in the following circumstances:</i></p> <ul style="list-style-type: none"> - <i>Where there is a high probability of a risk to that staff member’s safety; and</i> - <i>It is unreasonable or impractical to collect it directly from the staff member.</i> <p><i>Custodians must ensure to verify the details with the staff member providing it. A data entry form may be developed to assist with this process.</i></p> <p><i>Regular requests for staff to confirm any changes to their mobile phone numbers and / or name will be distributed. Staff will be personally responsible for ensuring that they confirm any changes.</i></p> <p><i>Custodians responsible for entering information into any medium will only be expected to rely on the veracity of the information provided to them and will be responsible for correctly entering that information, as provided.</i></p>	Complies	
11	<p>Principle 11 – Security of personal information.</p> <p>Take care of the information and protect it against loss, modification, or unauthorised disclosure and other misuse. When no longer required either destroy or de-identify it.</p>	<p>Collection</p> <p><i>The agency will ensure that the collection of staff mobile phone numbers is carried out by nominated information custodians.</i></p> <p><i>Information custodians will be nominated by virtue of their substantive positions as follows:</i></p> <p><i>Governance and Communications team and / or ICT team to obtain, enter and maintain information in the Redcoal / Optus SMS notification system.</i></p> <p><i>Line managers, office site managers and other delegated members of staff to collect, enter and maintain information stored in any other medium, including staff mobile phones, electronic data-bases and hard copy lists.</i></p>	Complies	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
		<p>Storage</p> <p><i>SMS notification system</i></p> <ul style="list-style-type: none"> • <i>The Optus SMS Suite employs Two Factor Authentication (2FA).</i> • <i>Further details about the security and privacy safeguards employed by the SMS notification system, refer to the Redcoal Privacy Policy.</i> • <i>To prevent the general disclosure of any other person's personal information, staff will not be able to view their information as entered into the active SMS notification system.</i> <p><i>Other storage media</i></p> <ul style="list-style-type: none"> • <i>An option will be provided for staff to consent for their phone numbers to be stored on nominated custodians' work mobiles. It is recommended that custodians provide a signed confidentiality statement in these circumstances.</i> • <i>For electronic information not stored in SMS notification system, it is recommended that secure folders in Objective are maintained.</i> • <i>Storage of hardcopy information is not recommended as this will prevent access to the information in an emergency if a custodian is not present in an office location during an emergency. If any staff who have provided their phone number do not wish for that information to be stored electronically, it must be stored in a secure location and only accessible by nominated custodians of that information.</i> <p>Destruction</p> <p><i>Staff will be responsible for advising nominated custodians when they no longer wish to have their personal details stored in any format. This will include advising when they are due to permanently leave the Office.</i></p> <p><i>Upon receipt of this notification, custodians will ensure that the relevant information is removed from all of the records they are responsible for.</i></p> <p><i>Governance and / or ICT will be responsible for ensuring the information is removed from the</i></p>		

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
		<i>SMS notification system, but no other media managed by other custodians.</i>		
12	<p>Principle 12 – Access to personal information</p> <p>People have a right to see their personal information noting exceptions apply, eg. FOI exemptions.</p>	<p><i>To prevent the general disclosure of any other person’s personal information, staff will not be able to view their information as entered into the active SMS notification system.</i></p> <p><i>If required, workarounds, such as system generated reports, edited screen shots etc will be considered.</i></p> <p><i>Similar actions may be relevant in allowing staff to access any other medium used to record staff personal mobile numbers (such as hard copy or electronic lists). Custodians responsible for maintaining these resources will determine how they manage requests to access this information.</i></p>	Complies	
13	<p>Principle 13 – Correction of personal information</p> <p>Agency must take steps to correct personal information held, ensure information is up to date, accurate, complete and not misleading.</p>	<p><i>The Office, via the Governance and Communication team and / or COO, will regularly request staff who have volunteered to provide their personal mobile numbers for the above purpose to update the information they have provided – name / mobile phone number – and also to advise if they no longer wish for these details to be retained and used for that purpose.</i></p>	Complies	

7. Privacy Management – Addressing Risks

Risk Mitigation Table												
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating							
1	<p>Security of external SMS notification system platform, Redcoal, being compromised ie via a hack / data breach and unauthorised release of information</p> <p>Risk category</p> <ul style="list-style-type: none"> Information systems Staff 	<p>The Optus SMS Suite employs Two Factor Authentication (2FA).</p> <p>Further details about the security and privacy safeguards employed by the system are contained in the Redcoal Privacy Policy.</p> <p>As at 17 October 2019, it is proposed that there will be no general access to the information contained in the system and that the information in this location will only be accessible by:</p> <ul style="list-style-type: none"> ICT Governance <p>In the event of a cybersecurity breach of information contained in the system, it is expected that the Office will rely on Optus / Redcoal to bear some or all of the risk outcome/s and treatment.</p> <p>The Office will locally address staff concerns regarding active privacy breaches and updates on treatment performed by third parties – ie: discussions / information sessions etc.</p>	Unlikely	Moderate	Medium							
2	<p>Unauthorised use of staff personal mobile numbers by other staff for purposes not related to notification of emergencies and / or other business disruptions</p> <p>Risk category</p> <ul style="list-style-type: none"> Compliance Information systems Staff Corporate responsibility Reputation 	<p>Manage by appropriate internal controls and regular monitoring:</p> <p>Policy / guidelines / notification</p> <ul style="list-style-type: none"> Guidelines and training for information custodians Information to all staff 	Possible	<p>Dependant on intent / consequence of use</p> <table border="1"> <tr> <td>For general contact</td> <td>Low</td> </tr> <tr> <td>Minor</td> <td rowspan="2">High</td> </tr> <tr> <td>For malicious use ie: harassment / cyber-bullying etc</td> </tr> <tr> <td>Major</td> <td></td> </tr> </table>	For general contact	Low	Minor	High	For malicious use ie: harassment / cyber-bullying etc	Major		
For general contact	Low											
Minor	High											
For malicious use ie: harassment / cyber-bullying etc												
Major												
3	<p>Unauthorised entry and storage of staff personal mobile</p>	<p>Manage by appropriate internal controls and regular monitoring:</p>	Possible	Minor	Medium							

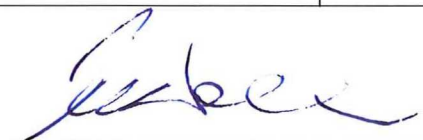
	<p>numbers and / or names in any medium used for the purposes of this project – ie SMS notification system, hardcopy and electronic records</p> <p>Risk category</p> <ul style="list-style-type: none"> • Compliance • Information systems • Staff • Corporate responsibility 	<p>Policy / guidelines / notification</p> <ul style="list-style-type: none"> • Guidelines and training for information custodians • Information to all staff 			
4	<p>Intended or unintended unauthorised disclosure of staff personal information to third parties, including other staff and / or external parties</p> <p>Risk category</p> <ul style="list-style-type: none"> • Compliance • Information systems • Staff • Corporate responsibility • Reputation 	<p>Manage by appropriate internal controls and regular monitoring:</p> <p>Policy / guidelines / notification</p> <ul style="list-style-type: none"> • Guidelines and training for information custodians • Information to all staff 	Possible	Moderate	Medium
5	<p>Staff not receiving notifications due to due to incorrect or outdated information being recorded in the SMS system or other medium used to record staff personal mobile numbers</p> <p>Risk category</p> <ul style="list-style-type: none"> • Information systems • Staff • Corporate responsibility 	<p>Manage by appropriate internal controls and regular monitoring:</p> <p>Policy / guidelines / notification</p> <ul style="list-style-type: none"> • Guidelines and training for information custodians • Information to all staff 	Possible	Minor	Medium

8. Recommendations

Ref	Recommendation	Agreed Y/N
R- 01	<p>For the sole purposes of notifying staff of an emergency affecting an Office location or other business disruption affecting its functions and / or actions, the Office will:</p> <ul style="list-style-type: none"> • Ask staff to voluntarily provide their personal mobile numbers for the stated purpose • Obtain, store and use voluntarily provided staff mobile numbers for the stated purpose 	

SIGNATURE

Rodney Lee Walsh, Chief Operating Officer and Privacy Delegate



Signature

Date 12.02.20