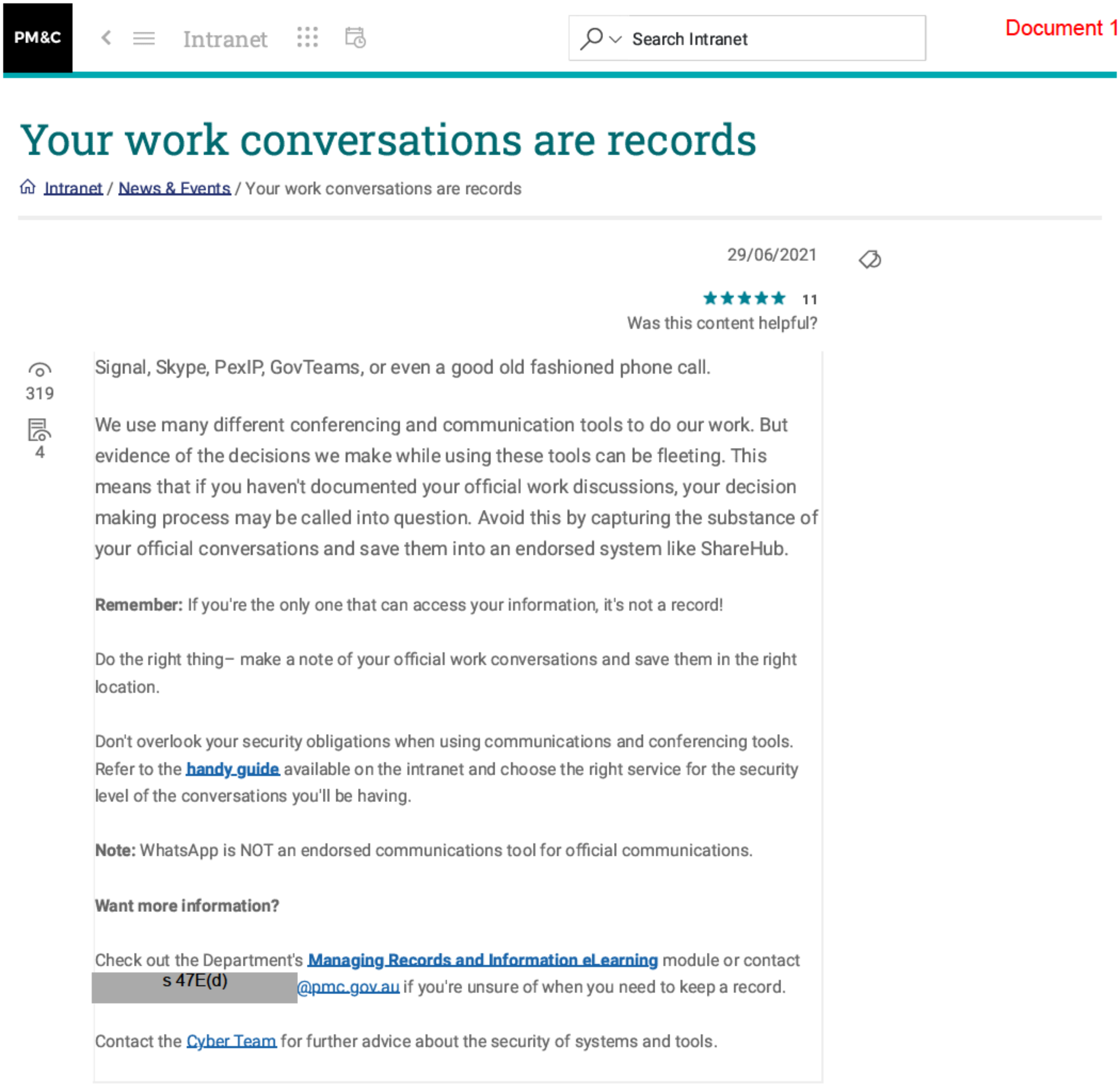
Document 1



# Your work conversations are records

Intranet / News & Events / Your work conversations are records

29/06/2021

★★★★★ 11
Was this content helpful?

Signal, Skype, PexIP, GovTeams, or even a good old fashioned phone call.

We use many different conferencing and communication tools to do our work. But evidence of the decisions we make while using these tools can be fleeting. This means that if you haven't documented your official work discussions, your decision making process may be called into question. Avoid this by capturing the substance of your official conversations and save them into an endorsed system like ShareHub.

**Remember:** If you're the only one that can access your information, it's not a record!

Do the right thing– make a note of your official work conversations and save them in the right location.

Don't overlook your security obligations when using communications and conferencing tools. Refer to the **handy guide** available on the intranet and choose the right service for the security level of the conversations you'll be having.

**Note:** WhatsApp is NOT an endorsed communications tool for official communications.

**Want more information?**

Check out the Department's **Managing Records and Information eLearning** module or contact s 47E(d) @pmc.gov.au if you're unsure of when you need to keep a record.

Contact the Cyber Team for further advice about the security of systems and tools.

Connect

Twitter
Facebook
YouTube
LinkedIn

Links

Prime Minister of Australia
Department of the Prime Minister and Cabinet
National Indigenous Australians Agency
indigenous.gov.au
federation.gov.au
Australian Parliament House
PM Transcripts
ABC News
BOM
GOLD
APSjobs

Help me find

Crisis and emergency
First Aid Officers
Health and Safety Representatives
Privacy at PM&C
Security
Workplace Respect Officers

Document 2

Australian Government
Department of the
Prime Minister and Cabinet

Chief Information Officer

# Policy on the use of consumer messaging apps

## *Private consumer messaging apps must not be used for the distribution or storage of official information. Online messaging services like WhatsApp, Signal, standard text messages (SMS), WeChat, iMessage, Telegram, Facebook Messenger, Snapchat, TikTok are not suitable to store official government records.*

Undeniably, private messaging apps and services are extremely useful and convenient for collaboration and information sharing. ***However, they are not authorised by the department to store or distribute official government information***.

Instead, staff should use **endorsed departmental services like email, ShareHub, PDMS, and Digital First** for the storage of official government information. This is because they have appropriate security and record keeping capabilities and are searchable for the purpose of supporting the FOI Act.

Unofficial or non-sensitive information suitable for use with these services is typically logistical or non-descript in nature. Simple examples of permitted conversations are things like coordinating travel with colleagues, agreeing to simple questions or coordinating major event logistics. Staff are reminded that using these types of services to discuss classified information is exactly like using any unknown or untrusted carrier services, such as phone conversations. Veiled references, oblique mentions and pre-agreed code words should always be used for any classified conversations, no matter the format or media, based on the sensitivity of the material and the location or service being used.

Typical departmental and ministerial scenarios are provided at the end of this document to help staff understand these requirements and provide context for their specific circumstances.

If this policy is breached and official Government information makes its way onto private apps, action must be taken immediately. *If you suspect any real or potential case of official information being distributed via these services, you must notify the Cyber Security team at* s 47E(d) *@pmc.gov.au for advice and action.* In the event there is an accidental sharing of official information, staff are required to extract and store this information in a searchable format on an official document storage application provided by the Department. Staff are then required to remove the information from the private app. Guidance will be provided on how to do so via the IT Service Desk or Cyber Security team.

If staff notice deliberate breaches (suspected or otherwise), staff must immediately notify the Cyber Security team at s 47E(d) s 47E(d)@pmc.gov.au.

Evidence of any staff member using these platforms to distribute official or sensitive information may be issued with a security breach notice and may possibly be further subject to further investigation under relevant legislation.

# Are there preferred private apps?

While PM&C does not yet endorse any private messaging app for official communication, it is preferred that staff use the Signal app over similar mobile communication platforms like WhatsApp for unofficial communications.

Regarding private use, at this time Signal would also be the preferred platform for staff communicating with family and friends, particularly when travelling. This is due to the verifiable open-source security model Signal has built in to the application, while other platforms have closed-source or unknown security models.

# Typical scenarios

Below are some typical scenarios PM&C users may encounter surrounding the use of commercial or consumer messaging platforms in their roles. For further information or you feel a particular scenario should be added to this document, please contact s 47E(d) @pmc.gov.au.

## Official information gets onto WhatsApp

Max has noticed that a work colleague within PM&C has sent official information via a WhatsApp group that Max is included in. What should Max do?

Max should contact the individual to ensure they have recorded the official information correctly on PM&C systems. Max should also contact the PM&C Cyber Security team to report a possible breach, providing as many details on the matter as possible. The original sender of the official information may be required to extract and transfer the WhatsApp conversation to PM&C systems so they are searchable and available during information or FOI requests.

## Team communication groups

Edith has recently been promoted to her first Assistant Secretary role and has been asked to join a Signal group that includes all other AS's in their Division. They was told it is used as a rapid way for Edith's FAS to contact direct reports. Edith knows these types of instant messaging applications shouldn't be used for official or sensitive discussions. Should Edith join this group?

It is fine for Edith to join this group and communicate with peers. This group should only be used for unofficial communications, like last minute meeting room changes, 'please contact me as soon as you get out of this meeting' texts or after-work catch-up's with colleagues. Like all participants Edith must ensure that her colleagues do not inadvertently send official or classified information via this platform.

## FOI requests

An FOI request has come to Faith's business area requesting all WhatsApp, Facebook Messenger and Signal conversations between staff members on the search term 'zeppelins'. What can Faith do to action this request fully, in compliance with the FOI Act?

Faith should contact the FOI team (foi@pmc.gov.au) and the identified decision maker for the request to discuss the appropriate course of action.

## Oblique references for classified material

Jeff does not have a lot of familiarity with dealing with classified material, but he now works in an area that deals with National Security and Cabinet information daily. His team makes extensive use of Signal to communicate – how does he ensure that he does not inadvertently disclose classified or sensitive material over this platform?

When discussing sensitive or classified material in an unknown or untrusted location, including cyber services, staff should ensure sensitive details are not revealed. Similar to how classified discussions must not occur where uncleared people can overhear, the language used via these online services should never directly refer to sensitive or classified material.

If Jeff needed to confirm that his supervisor would be notetaking during an upcoming Cabinet meeting, he should not reference the fact that this meeting is actually a Cabinet meeting. Instead, he might ask '*Jill from level is asking you to confirm you're availability for the meeting on Wednesday morning.*' or '*Can you confirm you're available for that topic we discussed yesterday?*' or simply '*I have sent you an email with an urgent question – can you please look it up and confirm?*' All of these are suitable for sending via Signal or WhatsApp, but don't reveal the topic or attendees of the meeting in question.

## Official travel groups

Ita is in a logistics WhatsApp group that includes government staff involved with an official trip overseas later in the year. Ita notices that someone from another government agency is using the channel as a quick method of asking meeting topic and content questions of officers involved in this travel. What should Ita do?

Ita should notify the officer the conversation is likely to become official in nature and should continue on official email or other government endorsed systems. If the officer continues the behaviour, notify the PM&C Cyber Security team who will then contact the Security team at the agency that the original sender belongs to**.**

These messaging platforms are perfect for quick and easy communication with member of an international travelling party. Having external parties in the groups can help coordination and logistics, particularly if the party is spread over multiple hotels or locations. Care must be taken that no official decisions or information is imparted using these platforms by staff from any agency, even if a question lends itself to an official answer. If a question needs an official decision or update, users should move the conversation to email so there is a formal record of the answer.

## Communicating with the Prime Minister's Office

Min is a PM&C EL2 and has been asked to join a WhatsApp group called 'Strategic Policy' that includes staff from PM&C, DFAT and the Prime Minister's Office. Should Min join this group and is there anything Min should watch out for?

Min should contact the requestor to determine if any political discussions or official Government information is being communicated in the group. If so, Min should not join this Group. If not, it is fine for Min to join this group. Min should contact her manager if she suspects the group discussion is being used for official government purposes.

## Self-destructing messages

Eddie has discovered there is a 'self-destructing message' security feature in Signal. Should Eddie use this feature for increased security in groups and one-on-one discussions with work colleagues?

It is noted that under PM&C's Normal Administrative Practices (NAP) policy, the deletion of low-value and short-term information is permitted provided that information can be verified as not necessary or suitable for long term record keeping.

Items suitable for destruction under the PM&C NAP policy can be found on the intranet or via s 47E(d) s 47E(d) @pmc.gov.au.

For work related groups, it is preferred that Eddie does not enable the self-destructing messages feature in Signal or other communications platforms. If Eddie does decide that the NAP policy for low-value information is relevant to a Signal conversation, manual deletion of the items is preferred over the self-destructing message feature.

# Security Implications

Services which have not been tested or certified for use with Australian government information may contain security vulnerabilities. In a lot of cases, the end user licence agreement (EULA) of these products states that information shared using their systems can be shared with third parties, usually advertisers, but also foreign governments. This is a significant reason why PM&C recommends the use of Signal over WhatsApp.

Staff found to be using these communications services for the transmission of official and/or classified information may be issued with a formal breach, as per the PM&C ICT Security Policy. For official purposes staff should only use authorised instant messaging products (Skype for Business) and work issued email accounts (Outlook).

The availability of all official information should be limited to those who need to use or access the information to do their work, determined via the need-to-know principle. For further information on handling official information please refer to the Security Framework.

# Further information

If you have any questions about the use of these services, please contact the Cyber Security team via s 47E(d) @pmc.gov.au.

# Social media, messaging apps and online storage

Intranet / Enabling Services / Cyber Security / Social media, messaging apps and online storage

Cyber Security ✕

- Classifying and sending secure email
- Cyber Security Policy
- Electronic device policies for secure areas
- Electronic device security in a Working Your Way world
- Email auto-forwarding
- FAQ - Stay Smart Online Week
- ICT and Internet Usage Agreement
- Internet website filtering
- Overseas travel cyber security policy
- Password requirements
- Phishing
- Registering electronic items in secure areas
- Secure video and voice conferencing
- [redacted] s 47E(d)
- Social media and you
- Social media, messaging apps and online storage

@ [redacted] s 47E(d) @pmc.gov.au 01/12/2022

☆☆☆☆☆ 0

Was this content helpful?

416

6

## Instant messaging and personal email

The use of consumer messaging products like Skype, WhatsApp, Wickr, iMessage, Telegram, TikTok, WeChat, Slack, Facebook Messenger or any other messaging tool **must not** be used for the distribution of official information. [redacted] s 47E(d) this functionality has been superseded and replaced with the release of Teams.

Official information **must not** be emailed to an employee's personal e-mail accounts like Gmail or Hotmail.

These services may only be used for the transmission of **unofficial information** – coordinating groups during travel, organising timing for meetings, logistics planning, friendly chats with co-workers and family, etc.

If official information does make its way onto any of these platforms, staff are required to extract and store this information in a searchable format on ShareHub. This is to meet record keeping legislation and to ensure official decisions are recorded for FOI purposes. The IT Service Desk can help a staff member to perform this transfer if necessary. Staff found using these platforms to distribute official or sensitive information may be issued with formal security breach.

The PM&C Cyber Security teams preference is for staff to use Signal over similar mobile communication platforms like WhatsApp or iMessage for personal calls and messaging. This is due to the verifiable security model Signal has built in to the application which makes it a much more secure option for any type of communication. It's not to say these other options are not suitable for personal communications at all, just that Signal is has a more transparent privacy and security policy.

## Blocked apps

It should be noted that in order to protect PM&C systems and information, certain mobile applications are blocked or prevented from working on PM&C issued devices. These

Wickr; Slack; Facebook Messenger; OneDrive; Box; Dropbox; Google Drive; information security; Skype; WhatsApp; signal

### On this page

- Instant messaging and personal email
- Blocked apps
- Online document storage systems
- Security implications

### You might like

[redacted] s 47E(d) 497

Secure video and voice conferencing 376

apps are blocked only after a formal risk assessment process by the Cyber Security team, with sign off by the CIO.

## Online document storage systems

Online storage systems like OneDrive, Box, Dropbox or Google Drive **are not** permitted to be used for the transfer or storage of official information without a business request thorugh the Service Portal.

In some cases when dealing with external parties staff may be required to access files stored using these services. In these instances, a user should contact the ICT Service Desk to request access to the online storage facility. In most cases the file will be  downloaded by the Service Desk on behalf of the user, and then placed in a nominated folder.

Requests for ongoing access to these types of services are assessed by the IT Security Adviser (ITSA). It is important to include a detailed business case when requesting access to these services.

## Security implications

Services which have not been tested or certified for use with Australian government information may contain security vulnerabilities. In a lot of cases, the end user licence agreement (EULA) of these products states that information shared using their systems can be shared with third parties, usually advertisers.

Staff found to be using these services for the transmission of official and/or classified information may be issued with a formal breach, as per the PM&C ICT Security Policy. For official purposes staff should only use authorised instant messaging products (Teams and Jabba) and work issued email accounts (Outlook).

On occasion, PM&C may block the installation or use of certain applications or services on issued electronic devices, separate to what is permitted under the incidental personal use policy. These blocks are due to internal risk assessment processes and typically target high risk or controversial products that may cause reputational damage if found on PM&C assets. Access to these blocked applications may be requested by contacting s 47E(d)@pmc.gov.au if a legitimate business need has been identified.

The availability of official information should be limited to those who need to use or access the information to do their work. For further information on handling official information please refer to the Security Framework.

If you have questions about the use of these services, please contact the Cyber Security team via s 47E(d) [redacted]@pmc.gov.au

### Connect

Twitter
Facebook
YouTube
LinkedIn

### Links

Prime Minister of Australia
Department of the Prime Minister and Cabinet
National Indigenous Australians Agency
indigenous.gov.au
federation.gov.au
Australian Parliament House
PM Transcripts
ABC News
BOM
GOLD
APSjobs

### Help me find

Crisis and emergency
First Aid Officers
Health and Safety Representatives
Privacy at PM&C
Security
Workplace Respect Officers

Australian Government

Department of the Prime Minister and Cabinet

# PM&C Cyber Security Policy

Version 3.0

October 2022

Australian Government
Department of the Prime Minister and Cabinet

CYBER SECURITY

# PM&C Cyber Security Policy

## 1 SYNOPSIS

| DOCUMENT DESCRIPTION |
|---|
| This document details the cyber security and ICT requirements that must be adhered to when using PM&C information technology and communication systems. |

## 2 CONTACT DETAILS

### 2.1 Document Creation

s 22(1)(a)(ii)

[redacted]

### 2.2 Amendment, Review and Approval

s 22(1)(a)(ii)

[redacted]

s 22(1)(a)(ii)

[redacted]

s 22(1)(a)(ii)

[redacted]

## 3.6 Minimum Standards

Policies and standards are essential to the conduct of PM&C's business. The policies and standards applicable to the Australian Government are imposed as a result of the legislation under which the Government operates. Refer to the Protective Security Plan for details of applicable legislation.

The following legislation provides controls which **must** be addressed in the conduct of PM&C's business:

- *Crimes Act 1914;*
- *Public Service Act 1999;*
- *Privacy Act 1988;*
- *Freedom of Information Act 1982;*
- *Electronic Transactions Act 1999;*
- *Evidence Act 1995;*
- *Copyright Amendment Act 1984;*
- *Occupational Health and Safety (Commonwealth Employment) Act 1991*; and
- *Archives Act 1983*.

To provide guidance in the application of the legislative requirements the Australian Government has produced the following policy documents to assist agencies in addressing their responsibilities for the protection of official resources:

- The Protective Security Policy Framework (PSPF); and
- The Australian Government Information Security Manual (ISM).

In addition, elements of this policy are drawn from the APS Values and Code of Conduct and PM&C's Data Breach Response Plan (DBR Plan).

Employees and contractors **must** adhere to the standards in this policy in order to satisfy their employment responsibilities.

A policy control within this document with a '**must**' or '**must not**' requirement indicates that use, or non-use, of the control is mandatory. Special dispensation must be sought from the Chief Security Officer (CSO) to deviate from a policy control outlined in this document that includes the term '**must**'.

s 22(1)(a)(ii)

[redacted]

### 6.18.3 Instant Messaging

External instant messaging services like WhatsApp, iMessage, Facebook Messenger etc **must not** be used to distribute official information, and provisions have been put in place to prevent the use of most major external instant messaging communication platforms.

s 22(1)(a)(ii)

[redacted]

s 22(1)(a)(ii)

Users **must not** circumvent controls in place to use external instant messaging services.

Mobile messaging services like Facebook Messenger, iMessage, WhatsApp, Telegram or similar are not to be used for the distribution of official information. s 47E(d), though it is being phased out in favour of Teams. s 47E(d) to be stored in ShareHub as a record.

More information on these services and how to choose the best service for your needs can be found on the Intranet Cyber Security section.

s 22(1)(a)(ii)