Department of the Prime Minister and Cabinet

Privacy Impact Assessment on the case management system – independent complaints and support service for serious incidents

Addendum 1:

Privacy Impact Assessment on the PWSS Expansion – Anonymous Digital Reporting

May 2022

Contents

1 Introduction

1.1 Background and Purpose

This Addendum has been prepared by KPMG for the Parliamentary Workplace Support Service (**PWSS**). It supplements the Privacy Impact Assessment (**PIA**) report on the Parliamentary Workplace Support Service (formerly known as the Serious Incident Team or SIT) (**PWSS**) Case Management System on 19 August 2021 (**Initial PIA**) to meet the planned timeline for the System go live date (**Report**). On 27 October 2021 KPMG issued an updated PIA (**Updated PIA**) report to confirm the assessment of the Case Management System developed for the PWSS to provide an independent complaints and support service for serious incidents.

This Addendum Report (**Addendum 1**) documents the extended PIA that KPMG has now conducted on the expansion of the scope of PWSS services to include an anonymous digital reporting pathway through its website at www.pwss.gov.au (**Website**).

The expansion of the services responds to Recommendation 20 (c) and (d) of '*Set the Standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces*' that was delivered to the Attorney-General on 21 November 2021.

Addendum 1, together with the CMS PIA, supports the PWSS to meet its obligations under Part 3 of the *Privacy APP (Australian Government Agencies) Code 2017* (**APS Code**) and the Australian Privacy Principles (**APPs**) in Section 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**).

1.2 Approach

This Addendum should be read in conjunction with the CMS PIAs. The PIA methodology reflected in this Addendum is the same as used for the CMS PIAs. A more detailed background to the functions and use of the CMS and PWSS services is contained in the CMS PIAs.

As part of this PIA we have:

- Assessed how the introduction of the anonymous digital reporting capability (**DAR channel**) on the Website will impact the collection, use, disclosure and storage of personal information (including sensitive information);
- Interviewed the key stakeholders in PWSS as set out in **Appendix 12**.
- Reviewed the relevant documentation provided by PWSS as set out in **Appendix 3**.
- Assessed the privacy impacts and benefits of the introduction of anonymous digital reporting capability against the Privacy Act and the APPs.

1.3 Assumptions and Limitations

Addendum 1 does not seek to revisit the risks or recommendations in the CMS PIAs. The scope of services that the CMS PIAs covered included anonymous reporting via other channels. In undertaking this assessment, we have assumed that the recommendations outlined in the CMS PIAs have been implemented or are in the process of being implemented.

This extended PIA focusses on the APPs relevant to the introduction of the DAR capability and includes recommendations relevant to addressing the risks identified from the assessment against those APPs. It also reflects the privacy benefits from introducing the DAR channel.

1.4 Disclaimer

Addendum 1 has been prepared at the request of the PWSS in accordance with the terms of KPMG's applicable engagement contract and is solely for the purpose set out in Part 1.1. Addendum 1 is only for the information of the PWSS and is not to be used for any purpose not contemplated in the engagement contract, or distributed to any third party without KPMG Law's prior written consent.

Other than KPMG's responsibility to the PWSS, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this Addendum 1. Any reliance(s) placed upon Addendum 1 are the sole responsibility of that party. The information contained in Addendum 1 is of a general nature and is not intended to address the specific circumstances of any individual or entity.

2 Key Findings and Recommendations

2.1 Positive observations

The introduction of the DAR channel will not materially alter the functions and/or services currently offered by the PWSS. Notably, it simply provides an alternative pathway for individuals to engage the PWSS without identifying themselves if they choose (for example, as opposed to via telephone).

The handling of anonymous reports was addressed in the CMS PIAs and we are satisfied that the policies, documents and procedures that are currently in place will generally adequately manage the addition of the DAR channel, subject to the recommendations below.

2.2 Risks and recommendations

We have not identified any high risks associated with the current procedural documentation being used by the PWSS. Because the DAR channel is an expansion of the PWSS' functions, some amendments are required to be documented, such as to the PWSS Privacy Policy, the Anonymous and Bystander Reports Factsheet and the privacy collection notices.

We have presented our recommendations in mark up within the relevant documents. Please see **Appendix 1** for soft copies of the marked-up documents.

2.2.1 Summary table of key risks and recommendations

APP	Risk	Risk Rating	Recommendations
APP 1	**Risk 1** Because of the addition of the purpose-built DAR channel, there is a risk that the Privacy Policy does not yet adequately explain an individual's ability to engage the PWSS anonymously across all channels and the consequences of this. Individuals should also understand how the information they submit through the DAR channel on this basis will be handled and relevant consequences to ensure transparency.	**Low**	Amend the Privacy Policy to provide greater clarity around an individual's ability to report anonymously and the consequences, including how their information will be used. Suggested amendments to the Privacy Policy have been provided by KPMG and accepted by PWSS. .
APP1	**Risk 2** There is a risk that the current Anonymous and Bystander Reports Factsheet does not clearly address the ability of bystanders to remain anonymous when making reports via the DAR channel.	**Low**	Amend the existing 'Anonymous and Bystander Reports Factsheet' to provide greater clarity around a bystander's ability to report anonymously. Suggested amendments to the Anonymous and Bystander Reports Factsheet have been provided by KPMG and accepted by PWSS.
APP1	**Risk 3** The framework of policies, procedures and processes that the PWSS has implemented does not effectively cover the DAR function including data flows, complaints, access and correction requests.	**Medium**	Review the data flows from the DAR channel through the CMS (See data flows explained in Section 4 below) to ensure the data is handled consistently with the data that is collected through other anonymous channels and the procedures for handling access and correction requests as well as privacy complaints from individuals who have used the DAR channel enables individuals to exercise their rights as far as possible. The Digital Anonymous Reports Protocol sets out the process that case workers are to follow upon receiving a report through the DAR channel. This sets out the requirements for, amongst other things, what information is recorded, what reports are responded to, and how the data within a report is collected and managed. This document should ensure data collected through the DAR channel is handled consistently with data collected through other anonymous channels.

APP	Risk	Risk Rating	Recommendations
APP 2	**Risk 1** Individuals wishing to make an anonymous report do not remain so because they submit personal information by identifying themselves or by becoming reasonably identifiable through the information they provide in the free-text box or the contact details.	**Medium**	2.1 A clear disclaimer is displayed before an individual clicks 'submit report'. KPMG has prepared suggested draft wording which has been accepted by PWSS. 2.2 The functionality of the 5000 character limit against the DAR design principles be reassessed in three to six months' time to determine whether the limit remains appropriate in the context of these considerations. 2.3 Ensure the privacy and confidentiality of those who choose to remain anonymous when reporting though the DAR channel is maintained during the process unless the individual elects to identify themselves
APP 3	**Risk 1** The current method by which individuals submitting reports agree to proceed, having read the privacy collection notice and privacy policy, risks not confirming consent to collect sensitive information if that is provided.	**Medium**	The Privacy Collection Notice is amended to refer to sensitive information and that the process captures consent. Suggested amendments to the Privacy Collection Notice have been provided by KPMG and accepted by PWSS.
APP 4	**Risk 1** Given the accessibility and ease of the DAR channel on the Website, there is a higher risk that anonymous reports or information included in the reports may be unsolicited where they do not relate to a serious incident that PWSS services support.	**Low to Medium**	The Digital Anonymous Reports Protocol should provide clear guidance to help PWSS staff determine whether each report submitted relates to a serious incident, and otherwise whether: it relates to PWSS's functions and activities; or the record of the report should be deleted in accordance with the records management process.
APP 5	**Risk 1** Because of the addition of the purpose-built DAR channel, there is a risk that the current Collection Notice #1 does not adequately explain an individual's ability to engage the PWSS anonymously. This could result in individuals misunderstanding their right to engage the PWSS anonymously and receive assistance and support on that basis.	**Low**	Amend Collection Notice #1 notice to provide greater clarity around an individual's ability to report anonymously. Suggested amendments to the PWSS Collection Notices have been provided by KPMG and accepted by PWSS.
APP 6	**Risk 1** Individuals may not understand how their reports will be used given they are anonymous and may not include personal information and they may not have any interaction with the PWSS.	**Low**	KPMG has provided amendments to the Privacy Policy to make clear how the anonymous reporting will be used for specific purposes. The amendments have been accepted by the PWSS.

APP	Risk	Risk Rating	Recommendations
APP 10	**Risk 1** Given the anonymous nature of reports that may be submitted through the DAR channel and that PWSS may not interact with the submitters, there is a risk that the reports may be unfounded or inaccurate. This may lead to inconsistencies in the quality of information recorded against different case records and could impact the effectiveness and/or outcome of a workplace review should the report proceed to such a step.	**Low**	In mitigation of this, the prescribed fields within the CMS, and the range of targeted guidance and training work will assist to reduce the likelihood of errors or inconsistencies in data entry to a low risk. In accordance with existing PWSS procedures, all individuals wanting to progress their report to a workplace review should be identified and all claims/assertions should be validated for accuracy.
APP 11	**Risk 1** There is a risk that deleted emails containing personal or sensitive information may be recoverable from the 'Deleted Items' folder in Outlook. Where emails containing personal or sensitive information are not permanently deleted from the 'Deleted Items' folder, the PWSS may be in breach of their obligation under APP 11 to take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose related to the PWSS' functions.	**Low**	11.1 Continue with the planning and progression of the data breach response tabletop exercise. Scope the exercise to include a simulated compromise of the shared mailbox. 11.2 The PWSS should manage this risk through enactment of the Digital Anonymous Reports Protocol. This document clearly sets out that all Case Coordinators/other PWSS staff are required to permanently delete emails containing personal or sensitive information from the 'Deleted Items' folder in Outlook once a report from the DAR channel has been uploaded to the CMS (or deleted due to irrelevance).
APP 13	**Risk 1** Individuals may wish to correct the personal information contained in an anonymous report that the PWSS holds which may not be able to be verified due to the anonymity of a report	**Low**	The PWSS should have a process in place for noting a statement from the requestor with the record that reflects the corrections sought, without changing the original record.

3 Background

3.1 *Set the Standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces (2021)*

On 5 March 2021, the Independent Review into Commonwealth Parliamentary Workplaces (**Review**) was established by the Australian Government, with support from the Federal Opposition and crossbench. Conducted by the Australian Human Rights Commission and led by the Sex Discrimination Commissioner, the Review was asked to make recommendations to ensure that Commonwealth parliamentary workplaces are safe and respectful, and that the nation's Parliament reflects best practice in prevention and response to bullying, sexual harassment and sexual assault.

The Set the Standard: Report on the Independent Review into Commonwealth Parliamentary Workplaces (**Report**) was tabled in November 2021.

While the PWSS already has a process for the handling of anonymous reports (via telephone or email), the recommendation calls for expanding the scope to a digital reporting channel to further simplify the accessibility of anonymous reporting to the PWSS.

To implement the recommendations in the Report, the PWSS has developed three new pages on the Website with the objective of providing an easy-to-use linear process that is intended to meet or exceed applicable web accessibility standards[1]. It has also prepared further material and a set of FAQs to assist those wishing to make such reports. The layout and contents of these pages is explained in Section 4 below.

[1] Web Content Accessibility Guidelines (WCAG) 2.0 Level AA

4 Data flows – digital anonymous reports

- The DAR link will be accessible from the homepage of the Website:

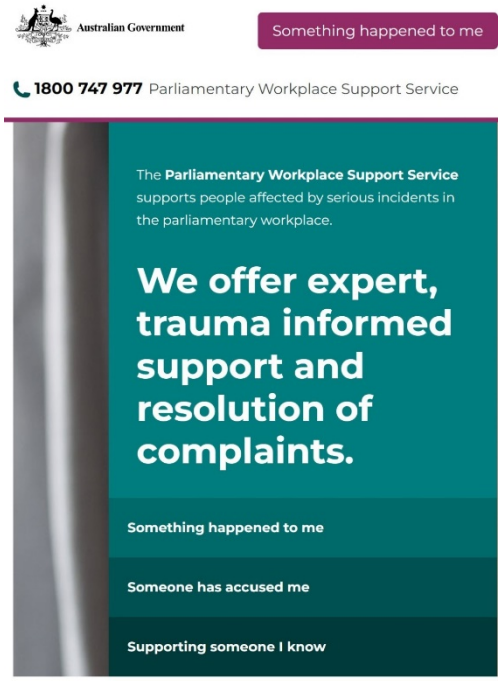

Figure 1 – *Suggested location for the link to the DAR channel on the PWSS homepage.*

An additional link to the DAR channel will also be made available from the "Making a Report" page on the Website.

- Once individual clicks this button to make an anonymous report, they will be taken to Page 1 which will provide information about anonymous reporting to the PWSS. Including:
  - A section titled: *What will PWSS do with an anonymous report?* This section also provides a link to the PWSS Privacy Policy.
  - A link to the PWSS privacy collection notices and a checkbox for the individual to acknowledge that they have read the Privacy Policy and collection notices and agree to proceed on that basis.
- Once the checkbox on Page 1 has been selected, only then will the individual be able to proceed to Page 2. Page 2 contains a free-text box into with the

individual is asked to input the details of their report and space for them to enter their contact details should they wish to be contacted by the PWSS.

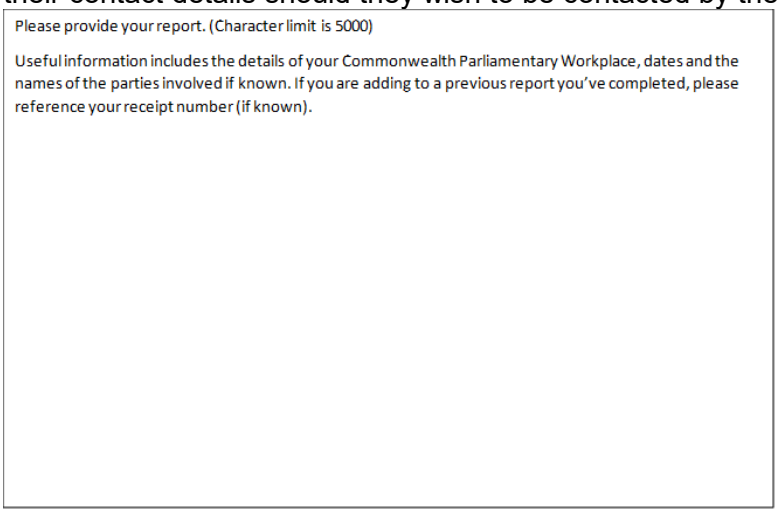

***Figure 2** – Free-text box on Page 2.*

  - Individuals are then asked if they wish to be contacted and if so if they wish to provide their contact details -if they say yes then they can choose to provide one or more of their preferred name, email and phone number, none of which are mandatory and are in free text
  - As a final step on page 2 - the 'submit' report button.
- Page 3 presents an acknowledgement of receipt and final information to the individual. A receipt number will be generated and presented on screen should the individual wish to make note of it for future interactions with the PWSS.
- On submission, the report will be sent via email to support@pwss.gov.au. The receipt number of the submission will be in the subject of email. For example "Subject: Anonymous Report #542".
- PWSS Case Coordinators will then review the email reports and create them as records in the CMS where they are related and relevant to the PWSS' functions. The accompanying emails will be exported to PDF and saved in the record's corresponding SharePoint folder as linked in the CMS.
  - Where reports have been submitted in an identifiable format (i.e. with the individual's name in the report, or in the contact details), the case will be created in the CMS in an identifiable manner (i.e. linked to the individuals name and unique identifier).
  - Where reports have been submitted anonymously, they will be entered into the CMS using the receipt number as the unique identifier.
  - Where reports contain details that are wholly unrelated to the function of the PWSS, the emails will be deleted from Outlook and no further action will be taken. The submitter will be notified that the report is unrelated to the function of the PWSS and no further action will be taken.
- After the report has been stored successfully as detailed above, the Case Coordinator will permanently delete the email containing the report from the support@pwss.gov.au account.
- The PWSS will proceed to handle all reports made through the DAR channel in accordance with its procedural documents which were reviewed as part of the CMS PIAs. As part of this process, in consultation with the Case Coordinator,

the Director of Case Coordination will assess the recommendations and provide endorsement for the agreed PWSS approach. Further consultation will occur with other PWSS staff as required.

5 Detailed Assessment

5.1 APP 1: Open and transparent management of personal information and privacy by design

The PWSS has developed practices, procedures and systems relating to its functions and activities that ensure it complies with the APPs and enable it to handle any complaints or inquiries about its compliance. This includes its External Privacy Policy (V1.0) (**Privacy Policy**).

The Privacy Policy already explains that individuals can engage with the PWSS anonymously or pseudonymously and the consequences of not providing personal information. The PWSS has also developed an Anonymous and Bystander Reports Factsheet which will be publicly available on the PWSS website.

Risk 1

Because of the addition of the purpose-built DAR channel, there is a risk that the Privacy Policy does not yet adequately explain an individual's ability to engage the PWSS anonymously across all channels and the consequences of this. Individuals should also understand how the information they submit through the DAR channel on this basis will be handled and relevant consequences to ensure transparency.

Low

Risk 2

There is a risk that the current Anonymous and Bystander Reports Factsheet does not clearly address the ability of bystanders to remain anonymous when making reports via the DAR channel.

Low

Risk 3

The framework of policies, procedures and processes that the PWSS has implemented does not effectively cover the DAR function including data flows, complaints, access and correction requests.

Medium

Recommendations

1.1 Amend the Privacy Policy to provide greater clarity around an individual's ability to report anonymously and the consequences, including how their information will be used. KPMG has made suggested amendments to the Privacy Policy, as marked up in the document titled 'External Privacy Policy V1.0 – KPMG Markup' at Appendix 1, which have been accepted by PWSS.

1.2 Amend the existing 'Anonymous and Bystander Reports Factsheet' to provide greater clarity around a bystander's ability to report anonymously. Suggested amendments to the 'Anonymous and Bystander Reports Factsheet – KPMG Markup' have been provided by KPMG and accepted by PWSS.

1.3 Review the data flows from the DAR channel through the CMS (See data flows explained in Section 4 below) to ensure the data is handled consistently with the data that is collected through other anonymous channels and the procedures for handling access and correction requests as well as privacy complaints from individuals who have used the DAR channel enables individuals to exercise their rights as far as possible. The Digital Anonymous Reports Protocol sets out the process that case workers are to follow upon receiving a report through the DAR channel. This sets out the requirements for, amongst other things, what information is recorded, what reports are responded to, and how the data within a report is collected and managed. This document should help ensure data collected through the DAR channel is handled consistently with data collected through other anonymous channels.

5.2 APP 2: Anonymity and pseudonymity

At present, individuals have the option to engage with the PWSS anonymously (or by using a pseudonym) via the existing contact channels (i.e. via email and via telephone). The process for this and how they are handled, is outlined in the CMS PIAs.

The introduction of the DAR capability will provide another avenue whereby individuals can engage the PWSS anonymously (or by using a pseudonym). The DAR capability will be implemented via the introduction of three new website pages to be located on the Website. Refer to Section 4 for a detailed explanation of the data flows.

The introduction of this DAR channel will not substantially change the way in which anonymous reports are currently being handled by PWSS Case Coordinators. That is, the PWSS Procedures Referrals and Intake document which instructs PWSS Case Coordinators on how to set up a client record when an individual wishes to remain anonymous; and the PWSS CMS – User Guide v1.1, which contains a section explaining how Case Coordinators can create anonymous client records in the CMS, still apply to reports made via the DAR channel.

Because of the nature of the DAR channel, there are however, some differences in the way reports are collected from individuals compared to the existing engagement channels (i.e. via email or telephone). Specifically, individuals will be given a free-text box (refer to Figure 2) where they are asked to provide their report, including useful details such as:

- the details of their Commonwealth Parliamentary Workplace;
- the dates and the names of the parties involved, if known; and
- if adding to a previous report, the receipt number of that previous report.

The character limit of the free-text box is currently set to the maximum of 5000 characters.

There is also an option for individuals to leave their contact details should they wish for the PWSS to contact them regarding their report. Individuals are permitted to provide a pseudonym in the contact details field should they wish to remain anonymous. We also assume they can still remain anonymous if they provide their telephone number only (which does not identify them).

Once a report is submitted via the DAR channel, an acknowledgement page and receipt number will be displayed to the individual and an email will be sent to the PWSS mailbox with the receipt number of the submission in the subject of the email. For example, “Subject: Anonymous Report #542”. Where the individual has not provided their identity in their report and/or contact details, Case Coordinators will review the contents of the report and enter it into the CMS following the protocols mentioned above for the lodgement of anonymous cases (i.e. by assigning a unique identifier). Where an individual has voluntarily chosen to identify themselves – either in the body of their report, or via the provision of their contact details – the report will be entered into the CMS as an identified case.

We note that individuals may choose to lodge their report via the DAR channel but also to voluntarily identify themselves in the process. Given that the details of the report they submit is done through a free text box, the amount and nature of the information they give may tend to identify them, or in fact do so. For example, where an individual provides the details of their Commonwealth Parliamentary Workplace and/or the dates and the names of the parties involved. However, it is understood that a lack of such information may result in it being impractical for the PWSS to handle or investigate an individual’s report.[2]

We also understand that there is no ability to submit attachments or PDFs with these reports. This will further mitigate the potential to identify an individual who makes an anonymous report.

Some cookies are used to collect information regarding interactions across all pages of the PWSS website. These are not specific to the DAR page(s). There are both Google Analytics and Imperva cookies used to collect data site wide. However, the cookies do not identify individual users or associate IP addresses with any other data. We consider the risks of identification from the abovementioned data to be low. However, we have provided recommendations which will work to further reduce any risks of identification below. On balance, it is clear from PWSS’ procedural documentation that an individual can remain anonymous when engaging the service and that processes are in place to ensure this anonymity can be managed unless an individual wishes to refer their case for workplace review.

Risk 1

Individuals wishing to make an anonymous report do not remain so because they submit personal information by identifying themselves or becoming reasonably

[2] OAIC guidance provides examples where it may be impracticable to deal with an individual who is not identified. Specifically, it may be impracticable to investigate and resolve an individual’s particular complaint about […] how the staff of an APP entity behaved unless the complainant provides their name or similar information.

identifiable through the information they provide in the free-text box or the contact details.

Medium

Recommendations

2.1 A clear disclaimer is displayed before an individual clicks 'submit report'. The disclaimer should help to minimises the collection of personal information as much as possible. The location, prominence, and design of disclaimer should ensure that it adequately captures the attention of the individual making the report. Suggested wording for a disclaimer is as follows:

> *'Please be aware that the information you include as part of your report may allow us to identify you. If you would like to remain anonymous, please ensure the information does not identify you. If you do enter personal including any sensitive information (such as your name and health status) in your report, your report will be treated as an identified report.'*

2.2 In landing on the functionality of the DAR design, PWSS had to carefully consider the purpose and function of the DAR function against the privacy risks associated with reporters providing irrelevant unsolicited information. In doing so, the PWSS considered several options including prescriptive answer fields or a smaller character limit. After internal deliberation, it was decided the DAR function would best facilitate anonymous reports under the DAR design principles by having a 5000 character limit.

It is recommended the functionality of the 5000 character limit against the DAR design principles be reassessed in three to six months' time to determine whether the limit remains appropriate in the context of these considerations.

2.3 Ensure the privacy and confidentiality of those who choose to remain anonymous when reporting though the DAR channel is maintained during the process unless the individual elects to identify themselves. The DAR function should prescribe under what circumstances an individual submitting a report will remain anonymous. Consistent with anonymous reporting through other channels, the DAR function and associated guidance and procedural documentation (including the Privacy Policy, SIT CMS – User Guide v1.2, PWSS Case Note Protocol, the Referrals and Intake procedure and Digital Anonymous Reports Protocol) should help ensure individuals can remain anonymous.

5.3 APP 3: Collection of solicited personal information

APP 3 permits personal information to be collected by an agency if it directly relates to or is reasonably necessary for one or more of the functions or activities. Personal information will generally only be collected with consent.

The DAR channel is designed to collect information in relation to serious incidents on an anonymous basis. As with the 'known' or non-anonymous reporting of incidents, the

DAR channel may result in the collection of information including information that falls within the definition of 'sensitive information' in Section 6(1) of the Privacy Act. Given the purpose for which the information is being collected under the anonymous reporting function, information collected could include sensitive information.

Information about an anonymous reporter will not be collected without the consent of that individual. Given the nature of DAR channel, it may also collect information about individuals such as accused parties without the knowledge of those individuals. It may be necessary for the anonymous reporter to provide this information in order to support the complainant in the management of their case.

For the purposes of the DAR channel, consent can be obtained when an individual proceeds through the website steps and submits a report. This is because the website is designed so that the individual cannot proceed to make a report unless the individual acknowledges they have read the privacy collection notice and Privacy Policy and agrees to proceed.

Risk 1

The current method by which individuals submitting report agree to proceed having read the privacy collection notice and privacy policy risks not confirming consent to collect sensitive information if that is provided.

Medium

Recommendation

3.1 We recommend that the wording is amended as follows:

> *By checking the box I acknowledge I have read the Privacy Collection Notice, I consent to PWSS collecting and processing the information I submit as explained in the Notice and Privacy Policy and agree to proceed.*

We have also included recommended amendments to explain the handling of anonymous reporting with other information that may be provided to support this statement.

The PWSS otherwise has policies in place that deal with the collection of personal information about other individuals and consent as follows:

- The Privacy Policy: explains that PWSS may collect personal information from third parties; outlines when this may happen in a manner that was solicited or unsolicited; and details how PWSS will obtain consent and the circumstances where consent may not be feasible or required.
- The Referrals and Intake procedure document provides detailed guidance to the PWSS staff about how to handle referrals from third parties, including that unsolicited information or information gathered without appropriate consents will not be recorded.
- The CMS includes consent gathering mechanisms which are explained in the PWSS SIT CMS - User Guide v1.2. The PWSS Templates_Intake Form with

Prompts provides guidance around consent and includes a consent capture box which must be marked with a yes for further information to be collected.

The above will also apply to the DAR function. In addition, the Digital Anonymous Reports Protocol should set out the process that case workers are to follow upon receiving a report through the DAR channel, amongst other things, what information is recorded, what reports are responded to, and how the data within a report is collected and managed.

5.4 APP 4: Dealing with unsolicited personal information

The new DAR channel is intended to make it easy and simply for users to submit anonymous reports. There is no triaging or discussion with a PWSS staff member (which may happen by phone) prior to a report being submitted and the report is described in the free text box provided. Once the report is received the PWSS will make a record of all reports that it will handle. If an anonymous complaint is submitted through the DAR and the subject matter is completely out of the scope of the functions of the PWSS or and/or not related to Commonwealth Parliamentary Workplaces, it will be deleted from the email server.

The PWSS has documents in place that provide guidance in relation to unsolicited information received through the DAR function. The Privacy Policy outlines how PWSS will handle unsolicited information, and the PWSS Referrals and Intake procedure document provides detailed guidance to the PWSS team about how to handle referrals from third parties, including that unsolicited information or information gathered without appropriate consents will not be recorded. The PWSS Templates_Intake Form with prompts also includes advice around consent.

Risk

Given the accessibility and ease of the DAR channel on the Website, there is a higher risk that anonymous reports or information included in the reports may be unsolicited where they do not relate to a serious incident that PWSS services support.

Low to Medium

Recommendations

4.1 The Digital Anonymous Reports Protocol should provide clear guidance to help PWSS staff determine whether each report relates to a serious incident, and otherwise whether: it relates to PWSS's functions and activities; or the record of the report should be deleted in accordance with the records management process.

5.5 APP 5: Notification of the collection of personal information

The PWSS has two privacy collection notices which are available on the Website:

1. The 'Individual accessing services of the PWSS – APP5 notice' which relates to individuals accessing the service, interacting with Case Coordinators and providing personal information in relation to an incident (Collection Notice #1); and
2. The 'Accessing the PWSS website – APP5 notice' which relates to the use of the Website by any visitors to that site, and how the Website collects personal information (Collection Notice #2).

Both collection notices are available under the 'privacy' section of the Website[3] and as determined by the CMS PIAs, the current notices meet the requirements of APP 5.

Having regard to the addition of the DAR capability to the Website, and the fact that the reporting channel specifically intends to provide an anonymous reporting function, we recommend that Collection Notice #1 be updated to ensure greater clarity around an individual's ability to report anonymously. See recommendation 5.1 below.

We understand that the Google Analytics and cookies being collected via the PWSS website apply on all pages of the site and do not identify individual users or associate IP addresses with any other data. The design process also states that there will not be a "Save and Return" option so that users do not feel that their IP address is being stored or that their draft information is able to be viewed (unless they submit their report). There have been no changes made to either the Google Analytics or cookies which are being collected on the PWSS site since the CMS PIAs. Accordingly, we consider that Collection Notice #2 continues to satisfy the requirements of APP 5 does not require amendment as a result of the addition of the DAR channel.

Risk 1

Because of the addition of the purpose-built DAR channel, there is a risk that the current Collection Notice #1 does not adequately explain an individual's ability to engage the PWSS anonymously. This could result in individuals misunderstanding their right to engage the PWSS anonymously and receive assistance and support on that basis.

Low

Recommendations

5.1 Amend Collection Notice #1 notice to provide greater clarity around an individual's ability to report anonymously. Suggested amendments to the PWSS Collection Notices have been provided by KPMG and accepted by PWSS.

5.6 APP 6: Use or disclosure of personal information

The Privacy Policy sets out the purposes of collection and the uses and disclosures the PWSS may make of personal information it collects. There will generally be no changes to the purpose of collection or uses and disclosures of personal information collected through the DAR function, including about third parties. The CMS PIAs

[3] PWSS Collection Notices, <https://pwss.gov.au/privacy#collection-notices>.

covered the planned and permitted uses and disclosures and handling the personal information of third parties collected through reports and the provision of its services.

However the purpose of enabling anonymous reporting reflects the Recommendation 20 in the Report - it is specifically for the purpose of contributing to the understanding of one off or systemic issues in Commonwealth Parliamentary Workplaces and informing actions that the PWSS undertakes to improve workplaces, including education and support.

Risk 1

Individuals may not understand how their reports will be used given they are anonymous and may not include personal information and they may not have any interaction with the PWSS.

Low

Recommendation

6.1 KPMG has suggested amendments to the Privacy Policy to make clear how the anonymous reporting will be used for the specific purpose. The proposed amendments have been accepted by PWSS.

5.7 APP 7: Direct marketing

N/A

5.8 APP 8: Cross-border disclosure of personal information

N/A

5.9 APP 9: Adoption, use or disclosure of government related identifiers

N/A

5.10 APP 10: Quality of personal information

APP 10 requires the PWSS to take reasonable steps to ensure that any personal information it collects and uses or discloses is accurate, up to date and complete and (for uses and disclosures) relevant.

Given the sensitivity of the information being collected and its potential impact, what will be considered reasonable steps for the PWSS to take may be more onerous to ensure the quality of the information being recorded in the CMS and used or shared. PWSS will attempt to validate the contents of a report submitted through the DAR reporting channel in accordance with the processes provided for in the Digital Anonymous Reports Protocol.

As explained in the CMS PIAs, case records are created and entered into the CMS in a heavily prescribed format. For example, there are limited free-text fields and there is guidance in the SIT CMS – User Guide v1.2, PWSS Case Note Protocol, the Referrals and Intake procedure and the Handling personal and sensitive information guidelines documents which advise Case Coordinators upon how to enter case records into the CMS to ensure consistency and quality.

Risk

Given the anonymous nature of reports that may be submitted through the DAR channel and that PWSS may not interact with the submitters, there is a risk that the reports may be unfounded or inaccurate. This may lead to inconsistencies in the quality of information recorded against different case records and could impact the effectiveness and/or outcome of a workplace review should the report proceed to such a step.

In mitigation of this, the prescribed fields within the CMS, and the range of targeted guidance and training work will assist to reduce the likelihood of errors or inconsistencies in data entry to a low risk.

Low

Recommendations

10.1 In accordance with existing PWSS procedures, all individuals wanting to progress their report to a workplace review should be identified and all claims/assertions should be validated for accuracy.

5.11 APP 11: Security of personal information

A detailed assessment of the security measures in place over the CMS are addressed in the CMS PIAs.

With the introduction of the DAR channel, we understand that submitted anonymous reports are sent to a shared mailbox which is currently in use by the PWSS. As assessed in the CMS PIAs, the shared mailbox is only accessible to authorised PWSS staff who have a business reason to access the information. In accordance with the CMS PIAs, we are satisfied that adequate access management protocols are in place to ensure effective control over the access to this shared mailbox.

Once anonymous reports are received to the shared mailbox, and provided that they are relevant to the PWSS' functions, Case Coordinators will create case records in the CMS. The corresponding email report will be exported to a PDF and will be saved in the record's respective SharePoint folder. The email will then be deleted from Outlook and in tandem, from the Microsoft Exchange Server.

Where a report is received via the DAR channel, but the contents of the report are deemed to be wholly unrelated to the PWSS' functions, the email will be deleted from Outlook without further action being taken.

We also note that a data breach response tabletop exercise is being planned and progressed at the time of writing this Addendum in accordance with the

recommendations in the CMS PIAs and will be scoped to include a potential mailbox compromise.

Risks

There is a risk that deleted emails containing personal or sensitive information may be recoverable from the 'Deleted Items' folder in Outlook. Where emails containing personal or sensitive information are not permanently deleted from the 'Deleted Items' folder, the PWSS may be in breach of their obligation under APP 11 to take reasonable steps to destroy of de-identify the personal information it holds once the personal information is no longer needed for any purpose related to the PWSS' functions.

Low

Recommendation

11.1 Continue with the planning and progression of the data breach response tabletop exercise. Scope the exercise to include a simulated compromise of the shared mailbox.

11.2 The PWSS should manage this risk through enactment of the Digital Anonymous Reports Protocol. This document clearly sets out that all Case Coordinators/other PWSS staff are required to permanently delete emails containing personal or sensitive information from the 'Deleted Items' folder in Outlook once a report from the DAR channel has been uploaded to the CMS (or deleted due to irrelevance).

5.12 APP 12: Access to personal information

Given the free-text and contact detail fields available for the DAR channel reporting, PWSS may end up collecting the personal information of an individual who had proceeded on the basis of an anonymous report. Accordingly, where personal information has been provided in the report and the PWSS has lodged it as an identified report in the CMS, they will be able to provide individuals access to their personal information in the same manner described in the CMS PIAs.

5.13 APP 13: Correction of personal information

We understand that PWSS does not seek to correct a record of an anonymous report received through the DAR channel as it will treat it as the record of the original report. It may also not have any opportunity to updated or add to a report of this kind. However, personal information about other individuals may be collected.

Risk

Individuals may wish to correct the personal information contained in an anonymous report that the PWSS holds which may not be able to be verified due to the anonymity of a report.

Low

Recommendation

13.1 The PWSS should have a process in place for noting a statement from the requestor with the record that reflects the corrections sought, without changing the original record.

6 Appendices

6.1 Appendix 1: Amended PWSS documents

Link	Document
x	Anonymous and Bystander Reports Factsheet
x	PWSS Privacy Policy
x	Collection Notices

6.2 Appendix 2: Stakeholders consulted

Name	Position/Department
Victoria Blakeley	Director, Legal and Governance PWSS
Nicoline Otieno	Senior Legal Officer, PWSS
Michael Douglas	Case Coordinator, PWSS

6.3 Appendix 3: Documents reviewed

1. Anonymous and Bystander Reports Factsheet Clean Version
2. External Privacy Policy V1.0 August 21 FINAL
3. PWSS Expansion – Anonymous Digital Reporting and Design Overview
4. Referrals and Intake Procedure
5. PWSS Case Note Protocol
6. SIT CMS - User Guide v1.2
7. Handling personal and sensitive information guidelines
8. Digital Anonymous Reports Protocol