Protocol for official searches for and extraction of documents

The purpose of this protocol is to set out the Attorney-General's Department's (the department's) procedures when conducting official searches for documents* in response to requests[#] including, but not limited to:

- audits
- investigations
- parliamentary processes (eg questions on notice)
- legal processes, including court orders for discovery, summonses or notices to produce
- reviews.

The protocol aims to provide a logical step-by-step procedure for searching for and extracting documents and to recording both the method of search and the outcome. It also aims to achieve a balance between a right to access information on the one hand and reasonable departmental controls on the other.

* Documents can include emails, minutes, submissions, letters, files, post-it notes, diaries, notebooks, reports, computer print outs, tapes or disks, text messages, plans, maps, photographs, microfiche, tape recordings, films, videotapes and metadata. Documents can be in various formats including, but not limited to, hard (paper) copy, electronic and digital. Draft documents are included within the FOI Act and need to be considered if within the scope of the request. [Adapted from Defence website: *Freedom of Information - What is a document for the purpose of freedom of information* http://www.defence.gov.au/foi/WhatIsADocument.asp]

[#] Requests can arise in different legal frameworks which may impose their own conditions. This may impact the search process. The terms of the particular request or court order/process should be carefully read and understood.

Search under the Freedom of Information Act

The department's procedures when conducting official searches for documents in response to requests under the *Freedom of Information Act* 1982 are outlined in the *AGD FOI Procedures Manual*, available on the department's Freedom of Information (FOI) intranet page. Those procedures are separate to the procedures dealt with under this protocol. Further advice on the application of the department's procedures in the context of FOI requests is available from the Director of the FOI and Privacy Section within the Office of Corporate Counsel.

Application to AGS

The senior person from the department with overall responsibility for responding to the request will send the request to AGS's Chief Operating Officer (COO) unless the scope of the request does not include AGS.

The AGS COO will deal with the request in accordance with the procedures set out in **Attachment A**. As AGS will normally hold documents in its role as legal advisor, the procedures take account of this role.

Search of departmental databases

The department's procedures require that any search of the department's databases, websites and spreadsheets undertaken by Information Division, will be in line with the department's *Standard Operating Procedure: Search and Extraction of Data for Audit & Investigation Purposes* (see **Attachment B**).

Records of such a search will be kept in accordance with the paragraphs under the *Reasonable search* and *Search declaration* steps below.

Please note that in applying the *Standard Operating Procedure*, the department **will not** access or retrieve emails between ministers and ministers' advisers, unless:

I. explicitly requested to include them, in writing, by the Minister or relevant Chief of Staff, or
II. legally compelled to provide access. In such an event the Secretary or a Deputy Secretary shall provide the approval for any search, with explicit reference to this protocol. The relevant Minister or Chief of Staff would be notified by the department, unless such notification is explicitly prevented by the legal order.

Searching for documents

Step 1: Determine the most appropriate business area to take responsibility for the search and coordinate AGD's response

1. The area responsible for the subject matter most closely connected to the documents sought and relevant senior officer(s) for that area eg authorising Band 2 officer(s) should be consulted and involved from the start of the process.
2. The relevant senior officer will decide who is going to manage the project and ensure a TRIM file is set up to keep a record of the steps taken (refer paragraph 15).
3. If necessary, the relevant senior officer will clarify scope of request. If a search request is difficult to understand, clarify the scope in writing (eg by email): what specifically is the applicant seeking access to? If the request is very broad it may be possible to negotiate to reduce the scope of the request. If the scope of the request cannot be clarified with the requestor, the responsible SES officers should be asked to sign off on the proposed interpretation of what is included / excluded from the request (this is important to ensure consistency when searching and when deciding which documents should be released).
4. The relevant senior officer will send out an email copy of the request to division heads / coordinators, including in AGS. The will give an indication of timeframe for initial response. Other divisions only need to respond if it is likely that they have documents relevant to the request. Other divisions may also be able to assist with suggested search terms/databases/timeframes/interpretation of the request etc.
5. The relevant senior officer will take responsibility for coordinating any consultation with other agencies – eg if sign off is needed to claim Public Interest Immunity for Cabinet-in-confidence documents; or if the documents concern the work of another agency who should be consulted or notified about their release, before they are released (refer paragraph 30).

Step 2: Where to search

6. In general, searches will be focused on documents held in the department's physical files or electronic IT systems and databases.

7. A list of the department's key searchable databases is at **Attachment C**. Please note – this list may not be exhaustive. As such, business areas with a likely involvement in the subject matter should be consulted for more information as they will have to search their own holdings, including in TRIM and Outlook (emails).
8. Information Services Section within Information Division can assist with complex searches in response to different types of requests. Consult with Information Division as early as possible if their help may be required.
9. Any searches of the department's databases, websites and spreadsheets undertaken by Information Division, will be in line with the department's *Standard Operating Procedure: Search and Extraction of Data for Audit & Investigation Purposes* (**Attachment B**).

Step 3: Request to search for documents

10. A request to search for and extract documents is needed before search action by Information Division can begin. A valid request would ideally:
    a. be in writing (including via email). If the request is made verbally, eg by telephone from a minister's staff member, send the requestor a follow-up email to confirm and clarify their request and its parameters (refer to (b) and (c) below). Ask for confirmation in writing (eg return email). Provide a copy to your SES manager
    b. provide information about the document(s) requested, including but not limited to, types of documents being sought, key search terms, date range of documents, possible author(s), and the reason for the request
    c. define the timeframe of the request: when is the information required and why (this is particularly important when the request is urgent and requires a fast turn-around).
11. If the request continues to be challenging, seek advice and guidance from your managing SES officer(s) and / or the Ministerial and Executive Support team in Strategy and Delivery Division (SDD).

Step 4 Analyse the search results

12. Each relevant division should examine the results of the search and identify pertinent documents from those results. Relevant documents should then be examined to determine whether further searching is required (eg because additional search terms are identified, a different database is identified as relevant, different business areas / individuals are identified as having an interest). Further consultation with other divisions may be needed.
13. Ensure that any additional documents referred to in relevant documents (eg attachments, related emails, meeting invitations) have all been located and examined for relevance.

Step 5: 'Reasonable' search

14. Generally you must do all that could reasonably be done to find the document(s) being requested.
15. To demonstrate that all reasonable steps have been taken, create an appropriate record of the search. The search record should include (at minimum):
    a. a copy of the original search request and any subsequent clarifications of the request
    b. locations/ offices/ databases / systems of which the searches were carried out
    c. identification of the person(s) who carried out the searches (name, position, business area)
    d. time spent searching each location
    e. results of the searches, ie number and description of documents located

f. where no documents were located, any known reasons why documents could not be located, eg never created, destroyed, archived or sent to another department
g. what steps were taken to locate any documents believed to be missing
h. whether relevant documents may have been disposed of, archived or transferred and if so, when and on what authority
i. any other locations at which you believe the relevant documents could possibly be found
j. for electronic searches, details of the parameters of each search: databases searched; search terms; date ranges applied (this could be partially satisfied by attaching print outs from databases or "screen dumps").

16. Record details about the search in a comprehensive search declaration. When the searches are extensive, set out the search results in a table for ease of future reference. Refer to **Attachment D** for an example template.

Sufficiency of search

17. The search required to locate a document can be complex. As explained above, you must do all that could *reasonably* be required of you to find the document in question.

18. In determining if all reasonable steps have been taken to find the requested documentation, consider the:

a. purpose for which the request for documents was made
b. content and relevance of the documents
c. existence and reasonably anticipated possible locations of the requested documents
d. steps already taken to locate the documents
e. consultation of all relevant persons within the organisation as to the possible existence of further documents
f. age of the documents
g. systems of file management during the relevant time period in issue and practices relating to document destruction or removal
h. commitments and workload of the personnel requesting the searches.
i. commitments and workload of the personnel undertaking the searches.

19. If a document cannot be located, the department needs to be able to demonstrate that all reasonable steps have been taken to locate the document.

20. If the document sought does not exist because it may never have been created, the department needs to satisfy itself that the document does not in fact exist, and if so satisfied, is not required to carry out any further steps to find the document.

21. If the document sought is believed to exist (to the extent it has been or should be in the department's possession) but it cannot be located, the department is required to carry out all reasonable steps to find the document before access to the document can be refused.

Step 6: Search declaration

22. A search declaration is a way of demonstrating compliance with the request to produce information as quickly and accurately as is reasonably possible. It should contain all the information from paragraph (15)(a)-(j) under Reasonable Search (above).

23. Include information about destroyed or deleted files if relevant, with an explanation as to why certain action has been taken. For example, an explanation that 'emails have been deleted because a hard copy was placed on the relevant file' or that 'the records or files have been archived (or destroyed) in accordance with an approved records disposal schedule'.

Example

I have searched the CAT database by (insert method) and located files ABC. I searched the DOG database but did not locate any information relevant to this request.

I searched the red and blue files in the file-room but found nothing of relevance. I also searched for files in the offsite archive storage and located files DEF which I considered to be relevant to the request. I have searched the email which contained relevant files GHI. In undertaking these searches I searched under the following search terms:

CAT; Cat; cAt; caT; C.A.T.; etc.

Attach table of results if appropriate (eg **Attachment D**).

24. File all details of searches and associated inquiries in an appropriately labelled TRIM sub-container for future reference. Apply appropriate controls to the TRIM sub-container.
25. Recording searches at the level of detail set out above may seem time-consuming. However, being able to provide detailed information about the searches conducted may help the requestor to fully understand the:
    - extent of searches undertaken for documents
    - reasons why any documents cannot be located.

    It may also result in the requestor being more satisfied with the search efforts of the department. The information can be relied upon later if the nature and extent of the search remains an issue.

Step 7: Quality assurance – providing the documents

26. Even when urgency and time constraints are important, it is essential to ensure that documents are reviewed thoroughly before provision to the requestor.
27. When reviewing the documents, ensure they fit the parameters of the original request. Remove any documents or parts of documents that fall outside the parameters, whether in terms of dates (timeframe) or issues (relevance).
28. Consider whether the volume or complexity of documents makes it most appropriate for the documents to be prepared, checked and provided in hard copy or electronic copy. This may include speaking with the requestor or party the documents are being provided to (for example, many courts prefer to work with electronic document production.)
29. Some documents or parts of documents may attract a privilege or immunity, even though they fit within the search terms. This can be a complex area. Consider whether the following privileges may apply and, if so, bring to the attention of the person coordinating the search for consideration and action:
    - Legal professional privilege, for example if the documents relate to legal advice or legal proceedings. Generally speaking the existence of these documents can be broadly referred to but details of the nature and content of the documents will not be disclosed and the department will seek a privilege from producing the documents.
    - Parliamentary privilege under s 16(3) of the *Parliamentary Privileges Act* 1987. If the document was prepared for the purpose of giving evidence in parliament or a presentation or submission to parliament, or is otherwise involved in the transaction of parliamentary business, parliamentary privilege may apply preventing the document from being relied upon in a court or tribunal. In those circumstances, the document might be able to be produced but the department as producing party would need to notify the other party that

the documents cannot be tendered or relied upon. It may be possible to negotiate the exclusion of such documents from the material produced especially when sought under court processes.

- Public interest immunity, such as for national security or Cabinet-in-confidence reasons. Often these documents are clearly marked with this protective marking or it is clear that they are sensitive documents from the context of the surrounding material.

30. If necessary, consult with other Commonwealth agencies or stakeholders with an apparent interest in the information to determine whether the information is sensitive and whether legal professional privilege or public interest immunities should be claimed. If the document request arises in the conduct of litigation, paragraph 7 of the *Legal Services Directions 2005* requires responding agencies to consult the agency with administrative responsibility for the immunity claim (eg within the Attorney-General's Department for parliamentary privilege related claims and the Department of the Prime Minister and Cabinet for Cabinet-related claims) before making the claim. In non-litigation contexts consultation is prudent and should be undertaken.
31. Ask another, appropriate, staff member to cross check that the search records match the documents being provided under the request.
32. The search records and related documents will need to be checked and approved by the relevant business area's SES Band 2 officer. In addition if the matter is sensitive, the First Assistant Secretary or Assistant Secretary, Strategy and Delivery Division can also be asked to provide assurance of the suitability of the documents. The approvals will be obtained in writing (at a minimum via email) and stored in TRIM with appropriate access controls applied.
33. Keep a copy of the documents being produced. Usually a schedule should be created which lists those documents provided, as well as those documents for which a privilege or immunity has been claimed (taking care to provide a general description only so as not to disclose privileged material in the schedule itself). This is useful both at the time of production and also later if needed to confirm precisely which documents were produced. The better the records kept at this stage, the easier it is to give that confirmation.
34. Following the relevant quality assurances and approvals, the documents can be provided as appropriate (keep a copy of documents provided). A record must be created which shows when the documents were sent to the requesting party, and stored in TRIM with appropriate access controls applied.
35. A search checklist is at **Attachment E**. Use the check list to ensure that you have followed these procedures adequately and provide it to the approving business area's SES Band 2 officer and /or the First Assistant Secretary or Assistant Secretary, Strategy and Delivery Division (as appropriate) at completion of the search.

Australian Government Solicitor

AGS GENERAL POLICY

GP-11 AGS protocol for official searches for and extraction of documents

Approved ***18 November 2015***
Sponsor *AGS Chief Operating Officer*

PURPOSE

1. This protocol set outs AGS's procedures when conducting official searches for documents* in response to requests# including:

   Audits

   Investigations

   Parliamentary processes (eg questions on notice)

   Legal processes, including Court orders for discovery, summonses or Notices to Produce

   Reviews

   Requests to respond to requests for documents received by the Attorney-General's Department (AGD).

   * Documents can include emails, minutes, submissions, letters, files, post it notes, diaries, notebooks, reports, computer print outs, tapes or disks, text messages, plans, maps, photographs, microfiche, tape recordings, films, videotapes and metadata. Documents can be in various formats including, but not limited to, hard (paper) copy, electronic and digital. Draft documents are included within the FOI Act and need to be considered if within the scope of the request.

   # Requests can arise in different legal frameworks which may impose their own conditions. This may impact the search process. The terms of the particular request or court order/process should be carefully read and understood.

2. This protocol does not deal with requests made under the *Freedom of Information Act 1982* or *Privacy Act 1988* which are covered under AGS general policies *GP-12 Handling FOI requests* and *GP-2 AGS privacy policy and guidelines* on the AGS policies page on OurAGS.

3. This AGS protocol is included in the AGD *Protocol for official searches for and extraction of documents* at Attachment A to that protocol.

SEARCH OF AGS RECORDS

4. Australian Government Solicitor (AGS) is a group within AGD providing legal services to government. As such, the great majority of our documents are created and held in our capacity as legal advisor. In many cases they are documents we hold on behalf of our clients and consideration will need to be given as to whether they are subject to claims for privileges or immunities such as Legal Professional

Privilege, public interest immunity or parliamentary privilege (see further below). In this protocol these documents are described as 'AGS client documents'.

5. AGS also holds documents dealing with its corporate governance and business arrangements. In this protocol these are described as 'AGS corporate documents'.

SEARCHING FOR DOCUMENTS

Step 1: Responsibility for the search and coordination of AGS's response

6. Any request for documents should be provided to the AGS Chief Operating Officer (COO).

7. If, for some reason, the COO is not able to receive or respond to the request, the Australian Government Solicitor will authorise an alternative person to be responsible for the response to the request. Steps said to relate to the COO in this document will relate to that alternative person.

8. The COO will consider whether the request is likely to require searches of AGS client documents and/or AGS corporate documents.

9. The COO will decide who will manage the response to the request (the search manager). The search manager will ensure a suitable record of the steps taken as set out in this protocol is established and stored on Worksite.

10. If necessary the COO or the search manager will clarify the scope of request. If a search request is difficult to understand, clarify the scope in writing (eg by email): what specifically is the requestor seeking access to? If the request is very broad it may be possible to negotiate to reduce the scope of the request.

11. The search manager will ensure AGS consults with clients or other agencies if needed – eg if Legal Professional Privilege is to be claimed (see below) or sign off is needed to claim Public Interest Immunity for Cabinet-in-confidence documents. The search manager should confirm with the COO who will be responsible for seeking client instructions and when this should occur. That person would make initial contact with the client to advise them that an official search request has been received, to outline AGS's proposed approach (including preliminary view about types of document likely to be covered by the request and any privileges), and to seek preliminary instructions to proceed in that manner.

Step 2: Where to search

12. Searches will be focused on documents held in AGS's physical files or electronic files (particularly for AGS client documents) or electronic IT systems and databases.

13. A list of AGS's key searchable locations and databases is set out in Table 1 below.

Searches for AGS client documents
Physical hard copy matter files
Elite
WorkSite
Law3000
Outlook
Objective
Consult with IT services regarding other searches that might be undertaken: Desktops; Personal drives/g drives
Secure storage of documents with security classifications
Backups of IT systems, kept by AGS IT Services
Searches for AGS corporate documents
Physical hard copy files
Elite
WorkSite
Law3000
Outlook
Objective
Backups of IT systems, kept by AGS IT Services

Table 1: Key searchable locations and databases for AGS searches

14. The list above is not necessarily exhaustive. The search manager should consider whether there are different areas of AGS with a likely involvement in the subject matter who should be consulted for more information as they will have to search their own holdings, including Outlook (emails) and any unfiled paper holdings eg notebooks.

15. Where the search may cover hardcopy or electronic security classified documents, in particular those held in secure storage, the search manager must consult the AGS Security Adviser and the AGS IT Security Adviser on the appropriate approach for conducting the search for, and handling of, such material. Further steps, such as client instructions, may be required before access to security classified documents can be given.

16. Backups created by AGS will usually need to be taken into account. For some requests, backups can be excluded from searches as not a reasonable search (see **Step 4: 'Reasonable' search** below) because of the significant cost and effort to access. Sometimes AGS will need to specifically identify in its response that it does not propose to review backups or seek the agreement of the requestor that backup searches are not required. It is likely that you will need to consult AGS IT Services about backups and obtain details about why backups are very difficult and time consuming to deal with in the context of the request.

17. AGS IT Services can also assist with complex searches in response to different types of requests. The search manager should consult with the National Manager AGS IT Services as early as possible if their help may be required.

18. Searches of AGS's electronic databases, websites and spreadsheets will be in line with any relevant AGS procedures operating from time to time.

19. The COO can authorise any necessary search of AGS records including files, electronic IT systems, and databases and secure storage facilities.

Step 3: Analyse the search results

20. The search manager should examine the results of the search and identify relevant documents from those results. Ask yourself again: is this document within the scope of the request?

21. Relevant documents should then be examined to determine whether further searching is required (eg because additional search terms are identified, a different database is identified as relevant, different areas / individuals etc are identified as having an interest).

22. Ensure that any additional documents referred to in relevant documents (eg attachments, related emails, meeting invitations etc) have all been located and examined for relevance.

Step 4: 'Reasonable' search

23. Generally the search manager must do all that could reasonably be done to find the document(s) being requested.

24. To demonstrate that all reasonable steps have been taken, create an appropriate record of the search. The search record should include (at minimum):

    a. a copy of the original search request and any subsequent clarifications of the request
    b. locations/ offices/ databases / systems of which the searches were carried out
    c. identification of the person(s) who carried out the searches (name, position)
    d. time spent searching each location
    e. results of the searches, ie number and description of documents located
    f. where no documents were located, any known reasons why documents could not be located, eg never created, destroyed, archived or sent to another department
    g. what steps were taken to locate any documents believed to be missing
    h. whether relevant documents may have been disposed of, archived or transferred and if so, when and on what authority
    i. any other locations at which you believe the relevant documents could possibly be found
    j. for electronic searches, details of the parameters of each search: databases searched; search terms; date ranges applied (this could be partially satisfied by attaching print outs from databases or 'screen dumps').

25. Record details about the search in a comprehensive search declaration (see **Step 5: Search declaration** below). When the searches are extensive, set out the search results in a table for ease of future reference. Refer to Attachment AGS1 for an example template. Where the search manager seeks the assistance of other areas of AGS in conducting the search, the search manager may ask those areas to record their search details in a similar fashion as input to the search manager's records and search declaration.

Sufficiency of search

26. The search required to locate a document can be complex. As explained above, the search manager must do all that could *reasonably* be required of them to find the document in question.

27. In determining if all reasonable steps have been taken to find the requested documentation, consider the:

    a. purpose for which the request for documents was made
    b. content and relevance of the documents
    c. existence and reasonably anticipated possible locations of the requested documents
    d. steps already taken to locate the documents
    e. consultation of all relevant persons within AGS as to the possible existence of further documents
    f. age of the documents
    g. systems of file management during the relevant time period in issue and practices relating to document destruction or removal
    h. commitments and workload of the personnel requesting the searches.
    i. commitments and workload of the personnel undertaking the searches.

28. If a document cannot be located, AGS needs to be able to demonstrate that all reasonable steps have been taken to locate the document.

29. If the document sought does not exist because it may never have been created, AGS needs to satisfy itself that the document does not in fact exist, and if so satisfied, is not required to carry out any further steps to find the document.

30. If the document sought is believed to exist (to the extent it has been or should be in AGS's possession) but it cannot be located, AGS is required to carry out all reasonable steps to find the document before access to the document can be refused.

Step 5: Search declaration

31. A search declaration is a way of AGS and the search manager demonstrating compliance with the request to produce information as quickly and accurately as is reasonably possible. It should contain all the information from paragraph 24(a)-(j) under **Step 4: 'Reasonable' search** (above).

32. Include information about destroyed or deleted files if relevant, with an explanation as to why certain action has been taken. For example, an explanation that 'emails have been deleted because a hard copy was placed on the relevant file' or that 'the records or files have been archived (or destroyed) in accordance with an approved records disposal schedule'.

    Example

    I have searched the CAT database by (insert method) and located files ABC. I searched the DOG database but did not locate any information relevant to this request.

    I searched the red and blue files in the file-room but found nothing of relevance. I also searched for files in the offsite archive storage and located files DEF which I considered to

be relevant to the request. I have searched the email which contained relevant files GHI. In undertaking these searches I searched under the following search terms:

CAT; Cat; cAt; caT; C.A.T.; etc.

Attach table of results if appropriate (eg Attachment AGS1).

33. File all details of searches and associated inquiries in an appropriately titled file for future reference. Apply appropriate controls to that file.

34. Recording searches at the level of detail set out above may seem time-consuming. However, being able to provide detailed information about the searches conducted may help the requestor to fully understand the:

- extent of searches undertaken for documents
- reasons why any documents cannot be located.

It may also result in the requestor being more satisfied with the search efforts. The information can be relied upon later if the nature and extent of the search remains an issue.

Step 6: Quality assurance – providing the documents

35. Even when urgency and time constraints exist, it is essential that the search manager ensure that documents are reviewed thoroughly before being provided to the requestor.

36. When reviewing the documents, ensure they fit the parameters of the original request. Remove any documents or parts of documents that fall outside the parameters, whether in terms of dates (timeframe) or issues (relevance).

37. Consider whether the volume or complexity of documents makes it more appropriate for the documents to be prepared, checked and provided in hard copy or electronic copy. This may include speaking with the requestor or the party the documents are being provided to (for example, many courts prefer to work with electronic document production.)

Consulting the client and any privileges or immunities

38. AGS will need to seek instructions from its relevant client before taking any steps in relation to producing AGS client documents.

39. Some documents or parts of documents may attract a privilege or immunity, even though they fit within the search terms. Consider whether the following privileges or immunities may apply and, if so, how it is proposed to deal with the documents.

- Legal professional privilege – for example if the documents are AGS client documents. These might relate to copies of legal advice or documents in legal proceedings provided in AGS's role as legal advisor. Generally speaking a schedule of these documents should be prepared so the existence of these documents can be broadly referred to but details of the nature and content of the documents will not be disclosed. AGS will seek a privilege from producing the documents.
- Parliamentary privilege under s 16(3) of the Parliamentary Privileges Act 1987. If the document was prepared for the purpose of giving evidence in parliament or a presentation or submission to parliament, or is otherwise involved in the

transaction of parliamentary business, parliamentary privilege may apply preventing the document from being relied upon in a court or tribunal. In those circumstances, the document might be able to be produced but AGS as producing party would need to notify the other party that the documents cannot be tendered or relied upon. It may be possible to negotiate the exclusion of such documents from the material produced especially when sought under court processes. AGD (Office of Constitutional Law), as the responsible agency for parliamentary privilege, should be consulted before any claim for parliamentary privilege is made.

- Public interest immunity – such as for national security or Cabinet-in-confidence reasons. Often these documents are clearly marked with this protective marking or it is clear that they are sensitive documents from the context of the surrounding material. If these are AGS client documents, the responsible person will need to ensure that we make inquiries with the client before taking any steps.

40. Privileges and immunities can be complex areas and the search manager should review other AGS procedures for dealing with them. If any claim for privilege or immunity arises, the search manager must consult with the Chief Solicitor Dispute Resolution or Deputy Chief Solicitor Dispute Resolution.

41. It may be necessary to consult with other Commonwealth agencies or stakeholders with an apparent interest in the information to determine whether the information is sensitive and whether legal professional privilege or public interest immunities should be claimed. If the document request arises in the conduct of litigation, paragraph 7 of the *Legal Services Directions 2005* requires responding agencies to consult the agency with administrative responsibility for the immunity claim (eg within the Attorney-General's Department for parliamentary privilege related claims and the Department of the Prime Minister and Cabinet for Cabinet-related claims) before making the claim. In non-litigation contexts consultation is prudent and should be undertaken. For AGS client documents, instructions from the client will be needed before discussing the client's documents with another agency.

Producing the documents

42. The search manager must keep a copy of the documents being produced. Usually a schedule should be created which lists those documents provided, as well as those documents for which a privilege or immunity has been claimed (taking care to provide a general description only so as not to disclose privileged material in the schedule itself). This is useful both at the time of production and also later if needed to confirm precisely which documents were produced. The better the records kept at this stage, the easier it is to give that confirmation.

43. The search manager should then present the documents to be produced to the COO for final approval to release. A checklist of potential steps required by this protocol is provided at Attachment AGS2. The completed checklist should also be provided to the COO.

44. The documents can be provided as appropriate. A record must be created which shows when the documents were sent to the requestor, and a copy filed on Worksite with appropriate access controls applied.

Record of document search – sample template

Record of Document Search [Title of Search] [Date of Search]							
Date	**Time taken**	**Name of officer**	**Position**	**Locations searched**	**Description of searches conducted/action taken**	**Result of searches**	**Comments/reasons why not located**

Search declaration

Example

I have searched the CAT database by (insert method) and located files ABC. I searched the DOG database but did not locate any information relevant to this request.

I searched the red and blue files in the file-room but found nothing of relevance. I also searched for files in the offsite archive storage and located files DEF which I considered to be relevant to the request. I have searched the email which contained relevant files GHI. In undertaking these searches I searched under the following search terms:

CAT; Cat; cAt; caT; C.A.T.; etc.

Attach table of results if appropriate (eg Attachment AGS1).

Checklist – protocol steps followed in conducting search of AGS records

Search manager

Prepared by:

Position:

Date:

Step 1 – Responsibility for the search and coordination of AGS's response	**Date**	
COO or delegated person receives the request		☐
COO considers whether AGS client documents or AGS corporate documents required to be located		☐
Search manager identified		☐
Search manager establishes record in WorkSite – with appropriate access controls		☐
Clarify and confirm search scope/parameters with requestor (if required)		☐
Saved final scope/parameters in WorkSite file		☐
Determined who is responsible for contact with client		☐
Contact with client to advise request has been received, proposed AGS approach (including preliminary view about types of document likely to respond and any privileges) and seek instructions to proceed in that manner.		☐
Step 2 – Where to search		
Identify the physical files, databases or other electronic systems to be searched		☐
Consulted with business area(s) responsible for subject matter to confirm any additional sources of relevant documents (eg individual email accounts, notebooks)?		☐
Does the request cover documents with security classifications that might be held in secure storage? Consult with AGS Agency Security Adviser and AGS IT Security Adviser Should you seek instructions before any steps are taken in relation to reviewing these documents?		☐
Asked AGS IT Services for help with complex searches		☐
Step 3 – Analysis of search results		
Examine results of searches and identified relevant documents. Ask yourself again at this point: is this document within the scope of the request?		☐
Consider if further searching and / or consultation with other business areas needed		☐
Locate and examine any additional documents or attachments referred to in relevant documents		☐
Steps 4 and 5 – Reasonable search & record keeping		
Demonstrate compliance with the request to produce information as quickly and accurately as reasonably possible. Create appropriate search record document– see steps set out at paragraph 24(a) – (j) and Attachment AGS1		☐
If a document could not be located, demonstrate that all reasonable steps were taken to locate the document		☐
Took all reasonable steps to find the requested document(s) – consider the factors at		☐

paragraph 27(a)-(i)		
Keep records of searches and results in WorkSite		☐
Step 6: Quality assurance & providing the documents		
Review the documents thoroughly before provision to the COO to ensure the documents fit the parameters of the original request. Are they relevant, do they fit within the timeframe of the requested material?		☐
Prepare, check and provide the documents in hard copy or electronic copy depending on the volume or complexity of documents		☐
Consider whether any documents attract a privilege or immunity. Consult with Chief Counsel Dispute Resolution or Deputy Chief Counsel Dispute Resolution		☐
Consult any external agency or other third party regarding any proposed privilege or immunity claim		☐
Claim for privilege or immunity made		☐
Keep a copy of the documents being produced		☐
Prepare a schedule listing those documents provided, as well as those documents for which a privilege or immunity has been claimed (taking care to provide a general description only so as not to disclose privileged material in the schedule itself)		☐
COO provided with copy of request, documents, schedule of documents and checklist to sign off readiness for production		☐
Created record showing when the documents were sent to the requesting party, and stored record in WorkSite with appropriate access controls applied		☐

Cleared by COO:

Date:

Comments:

Australian Government
Attorney-General's Department
Information Division

Standard operating procedure: search and extraction of data for audit & investigation purposes

Objective: To outline the framework and standard operating procedure (SOP) to be applied in responding to requests for data extractions (including sensitive data) to support audits, investigations or other similar activities.

Application: This SOP shall apply to all requests for data, regardless of scale/volume, which involve an external party seeking access to data created by another person.

In applying this SOP, the department will not access or retrieve emails between ministers and ministers' advisers, unless:

i. explicitly requested to include them, in writing, by the Minister or relevant Chief of Staff, or

ii. legally compelled to provide access. In such an event the Secretary or a Deputy Secretary shall provide the approval for any search, with explicit reference to this protocol. The relevant Minister or Chief of Staff would be notified by the department, unless such notification is explicitly prevented by the legal order.

STANDARD OPERATING PROCEDURE

The following processes shall be adhered to when responding to requests for retrieving data.

1. The requestor must be, at a minimum, an AGD SES Band 1 level officer, or the Director of the Governance Office (Strategy and Delivery Division).

2a. Where a valid request has been received by the Chief Information Officer or Assistant Secretary in Information Division, the task will be assigned to an Action Officer (in most instances, the Director, System Operations).

2b. Where a valid request has been received by non-SES staff within Information Division, and where it is unclear that Information Division's Executive have been made aware of the request, Information Division's Chief Information Officer and Assistant Secretary must be advised of the request, unless specifically requested not to by the First Assistant Secretary or Assistant Secretary, Strategy and Delivery Division, or the Assistant Secretary, People Strategy Branch.

3. The Action Officer must engage with the requesting area/requestor to take steps to clarify/clearly define the scope of the task, agree what systems and files will be searched, and develop an estimate of the work effort/time required to meet the request. Active consideration shall be given to information that should be excluded from the search and extraction.

4. The Action Officer will keep a record of the agreement (at a minimum via email), clearly indicating that both Information Division and the requesting party understand and agree to the scope of work. This approval must be stored in TRIM with appropriate access controls applied.

5. Where the estimated work effort is likely to exceed 5 days, or will require specialist expertise to be engaged to complete the work, the Action Officer shall discuss the potential for cost recovery (from the external requesting party) with the requesting area. Where necessary these discussions should be referred to the relevant SES officers.

6. Once task-scope and timeframe has been agreed, the Action Officer may assign the task to an Approved Staff Member - Refer to Appendix A for Approved Position Numbers.

    - Only two of these Approved Staff Members are permitted to access AGD system mailboxes and extract email information.
    - The Approved Staff Member may only access AGD system mailboxes in response to a specific request, and following authorisation from the department's security adviser, the Director of the Governance Office, First Assistant Secretary or Assistant Secretary, Strategy and Delivery Division, or the Assistant Secretary, People Strategy Branch.
    - If asked to extract emails from the system, the Approved Staff Member will view only the subject line, sender/addressee and date/time information and not the content.
    - Particular care must be exercised by the Approved Staff Members not to breach parliamentary privilege in the data extraction or data provision process.
    - All actions taken by the Approved Staff Members are logged. The logs are checked on a case-by-case basis in response to a specific requirement or investigation.
    - The Department's IT Network Systems Conditions of Access make it clear that any individual's use of AGD IT facilities that is without authority or excess of their authority may result in disciplinary and/or legal action.

7. Where it is determined that a staff member other than an Approved Staff Member is required to undertake the work, this shall be agreed in writing (at a minimum via email) with the Chief Information Officer (CIO), or First Assistant Secretary Strategy and Delivery Division or Assistant Secretary People Strategy Branch, in circumstances where the CIO has not been advised of the data extraction request (see paragraph 2b). This approval must be stored in TRIM with appropriate access controls applied.

8. Prior to commencing the data extraction the Approved Staff Member will create a location for the extracted data to be placed which can be accessed by the requesting officer and other staff approved by the requesting officer for the purposes of data review.

9. When the data extraction has been completed the Action Officer shall review the data for quality assurance purposes, to ensure that only data which matches the agreed data extraction parameters has been provided.

10. Upon completion of the quality assurance review, the Action Officer shall provide the data set to the nominated contact officer within the requesting area for assessment.

11. Line areas are to assess the data and with explicit approval from a SES level officer in the line area, indicate to the Action Officer those data items:

a. which fall within scope and can be released;
b. which fall outside of scope and must be removed from the data set, including for example, ministers' and advisers' emails

12. Data set remediation will be completed by the Action Officer and Approved Staff Member and the full data set returned to the requesting area for final review and confirmation of data set suitability. In addition, the First Assistant Secretary or Assistant Secretary, Strategy and Delivery Division will be asked to provide assurance of data set suitability at this time. Confirmation of data set suitability will be obtained in writing (at a minimum via email) and stored in TRIM with appropriate access controls applied.

13. The Approved Staff Member will transfer the final data set as appropriate for distribution. Records will be created which indicate when data was transferred from Information Division to an external party (either the requesting area or an external body such as the ANAO, for example), and stored in TRIM with appropriate access controls applied.

14. The Action Office must ensure that an electronic copy of the final data set is stored within a secure location in TRIM using the following naming convention:

    - matter descriptor – nature of authority (internal/external audit/investigation) – requesting officer name - file status (eg draft/final) – date finalised –

    for example:
    - Timekeeper audit data extraction by Information Division – internal EY audit – requested by Jane Doe - final – 7 May 2015; or
    - SAP access data extraction by Information Division – external ANAO audit – requested by Joe Bloggs - final – 7 May 2015.

Appendix A – Approved staff members – position numbers

For the purposes of this SOP Approved Staff Members will be those occupying the following position numbers:

PN 2500901 – System Engineer
PN 2502803 – Network Engineer
PN 2502916 – Assistant Director
PN 2500902 – Assistant Director
PN 2502225 – ITSA
PN 2502034 – ITSM

Checklist

Appropriate authority for request confirmed	☐
Advised CIO/AS if not otherwise aware	☐
Assigned task to Action Officer	☐
Request scope/parameters confirmed	☐
Finalised scope/parameters saved in TRIM	☐
Estimate of effort provided to requesting area	☐
Discussions re cost recovery finalised (where applicable)	☐
Task Assigned to Approved Staff Member for completion	☐
CIO approval for additional Approved Staff Members to complete work saved in TRIM	☐
Creation of location for data set for review purposes completed	☐
Quality assurance of extracted data set completed by Action Officer	☐
Data set provided to requesting area and record made in TRIM	☐
Requesting area confirms changes (where applicable)	☐
Request for changes (if applicable) saved in TRIM	☐
Data set amended and returned to requesting area for secondary review and record made in TRIM	☐
Amended data set provided to Assistant Secretary or First Assistant Secretary, Strategy and Delivery Division for final assurance	☐
Requesting area provides authority to release	☐
Assistant Secretary or First Assistant Secretary, Strategy and Delivery Division provides authority to release	☐
Authority to release saved in TRIM	☐
Record of provision of final data set to requesting area/external party saved in TRIM	☐
Final data set saved in TRIM using naming convention	☐

Core departmental information databases

TRIM

MyHub/SAP

Exec Corro/PDMS

Outlook

IRIS (specific application, but endorsed as an approved record keeping system)

Subject specific / managed data stores

These include but are not limited to:

Desktops

Personal drives/g drives

CommVault

Cobra

CLSIS

Firearms permits database

Auscheck

NSH database

Register of Approved Persons, Warrants and Other functions

Federal Offenders database

LRS/LRO

Various grants management systems

Sharepoint sites

Marcel

Audit database

Arts appointments register

Register of moveable cultural heritage

Register of cultural organisations

Spreadsheets

Data - AGD staff members

Aurion

DSU database

Active Directory

Record of Document Search [Title of Search] [Date of Search]								
Date	**Time taken**	**Name of officer**	**Position**	**Business Unit**	**Locations searched**	**Description of searches conducted/action taken**	**Result of searches**	**Comments/reasons why not located**

Checklist – Protocol steps followed in conducting search

Prepared by:
Position:
Date:

Checked by:
Position:
Date:

Step 1 – Determine the responsible / coordinating/ lead area and senior officer(s)	
Identified and advised lead business area	☐
Identified and consulted authorising / managing SES Band 2 officer(s)	☐
Created a dedicated TRIM container for record keeping for this search	☐
Clarified and confirmed search scope/parameters with requestor (if required)	☐
Saved final scope/parameters in TRIM file	☐
Emailed copy of request to all relevant Division Heads and coordinators	☐
Consulted portfolio agencies (if appropriate)	☐
Step 2 – Where to search	
Identified the physical files, databases or other electronic systems to be searched	☐
Consulted with business area(s) responsible for subject matter to confirm any additional sources of relevant documents (eg individual email accounts, notebooks)	☐
Step 3 – Request to search	
Asked Information Division for help with complex searches	☐
Provided Information Division a valid request to search for and extract documents: in writing; provided information about document(s) requested, and defined timeframe	☐
Searches performed by Information Division were in line with the department's *Standard Operating Procedure: Search and Extraction of Data for Audit & Investigation Purposes*	☐
Step 4 – Analysis	
Examined results of searches and identified relevant documents	☐
Examined relevant documents to determine if further searching and / or consultation with other divisions / business areas needed	☐
Located and examined any additional documents referred to in relevant documents, for relevance	☐
Step 5 – Reasonable search & record keeping	
Did all that could reasonably do to find the requested document(s)	☐
Created appropriate search record document (paragraph 18 (a)-(i))	☐
If a document could not be located, demonstrated that all reasonable steps were taken to locate the document	☐
Step 6 – Search declaration	
Demonstrated compliance with the request to produce information as quickly and accurately as reasonably possible (paragraph (15)(a)-(j))	☐
Created an appropriate search record (eg Attachment D)	☐
Step 7: Quality Assurance & providing the documents	
Reviewed the documents thoroughly before provision to the requestor to ensure the documents fitted the parameters of the original request	☐
Prepared, checked and provided documents in hard copy or electronic copy depending on the volume or complexity of documents	☐
Checked if any documents could attract a privilege or immunity, and made the person coordinating the search aware of these	☐

Consulted any external agency or other third party regarding any proposed privilege or immunity claim	☐
Keep a copy of the documents being produced	☐
Prepare a schedule listing those documents provided, as well as those documents for which a privilege or immunity has been claimed (taking care to provide a general description only so as not to disclose privileged material in the schedule itself)	☐
Another appropriate staff member cross checked that the search records matched the documents being provided	☐
Relevant business area's SES Band 2 officer checked and approved (in writing) the search records and related documents	☐
First Assistant Secretary or Assistant Secretary, Strategy and Delivery Division provided assurance of the suitability of the documents, if the request was particularly sensitive	☐
Created record showing when the documents were sent to the requesting party, and stored record in TRIM with appropriate access controls applied	☐