Attorney-General's Department

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 orders
- Reviews

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

* Please note: 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 exist in different legal frameworks which may impose their own conditions. This may impact the search process.

Search under the Freedom of Information Act

The department's procedures when conducting official searches for documents in response to request under the Freedom of Information Act 1982 are outlined in the *AGD FOI Procedures Manual*, available on the department's Freedom of Information (FOI) and Privacy Section's intranet page. Those procedures are separate to those 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.

Search of Departmental Databases

Any search of the department's databases, websites and spreadsheets that has to be undertaken by Information Division, will be performed in line with the department's *Standard Operating Procedure: Search and Extraction of Data for Audit & Investigation Purposes* (see Attachment A). Records of such a search will be kept in accordance with the paragraphs under Reasonable Search and Search Declaration 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.

A list of the department's key searchable databases is at Attachment B. 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. The Information Division should be consulted too. Information Services Section within Information Division can assist with complex searches of TRIM in response to different types of requests.

Searching for Documents

Request to search for Documents

1. A request to search for and extract documents is needed before search action can begin. A valid request would ideally:
    i. 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 (ii) and (iii) below). Ask for confirmation in writing (eg return email). Provide a copy to your SES manager.
    ii. 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
    iii. 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).
2. In general, searches will be limited to documents held in the department's physical files or electronic IT systems and databases. [A list of these is attached].
3. 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 continues to be challenging, seek advice and guidance from your managing SES officers and / or the Ministerial and Executive Support team in Strategy and Delivery Division (SDD)

Reasonable Search

1. Generally you must do all that could *reasonably* be done to find the document(s) being requested.
2. To demonstrate that a reasonable search for documents was conducted, create an appropriate record of the search. The search record should include (at minimum):
    a. 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 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 are 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. with respect to 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").

3. 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 C for an example template.

Search Declaration

1. 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 (2)(a)-(k) under Reasonable Search (above).
2. 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 schedule'*.

   Example
   I have searched the XYZ database by (insert method) and located files ABC. I searched the 123 database but did not locate any information relevant to this request.
   I searched the red and blue files in the storeroom but found nothing of relevance. I also searched for files in the offsite archive storage and located files 456 which I considered to be relevant to the application. I have searched the email which contained relevant files DEF. In undertaking these searches I searched under the following search terms:
   XYZ; Xyz; xYz; xyZ; X.Y.Z.; x.y.z.; etc.
   [Attach table (eg Attachment C) if appropriate]

3. 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.
4. 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 an applicant to fully understand the:
   - extent of searches undertaken for documents
   - reasons why any documents cannot be located.

   It may also result in the applicant being more satisfied with the search efforts of the department.

Sufficiency of search

1. 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.
2. In determining if all reasonable steps have been taken to find the requested documentation, consider the:
   i. content and relevance of the documents
   ii. existence and location of the requested documents
   iii. steps already taken to locate the documents

iv. consultation of all relevant persons within the organisation as to the possible existence of further documents
v. age of the documents
vi. systems of file management and practices relating to document destruction or removal
vii. purpose for which the request for documents was made
viii. commitments and workload of the personnel requesting the searches.
ix. commitments and workload of the personnel undertaking the searches.

3. 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.
    i. 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 all reasonable steps to find the document
    ii. If the document sought exists (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 documents before access to the document can be refused.

Quality Assurance

1. Even when urgency and time constraints are important, it is essential to ensure that documents are reviewed thoroughly before provision to the requestor.
2. When reviewing the documents, ensure they fit the parameters of the original request. Remove any documents that fall outside the parameters.
3. Ask another, appropriate, staff member to cross check that the search records match the documents being provided under the request.
4. 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.
5. Following the relevant quality assurances and approvals, the documents can be provided as appropriate. 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.

Attachment A

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 and Repositories

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**