



Outlook Quickparts used by the Central OIA inbox

The below wording is in use by the Central inbox. Please feel free to adopt any of these email templates you choose. Note however some wording in our quickparts is only included on a case by case basis. You will need to read carefully and decide whether all content is appropriate to your circumstances, and delete parts you do not need

Contents

- [Acknowledge OIA](#)
- [Allocate OIA](#)
- [Clarify/refine request scope](#)
- [Confirm clarified/refined request](#)
- [Consult with agency on transfer](#)
- [Notify requester of transfer](#)
- [Confirm transfer to the agency](#)
- [Notify transfer to the agency w/o consultation](#)
- [Notify/consult third party on request that includes their information](#)
- [Extend request timeframe](#)
- [Notify requester of decision](#)
- [Redirect Archives NZ research request](#)

Acknowledge OIA

Tēnā koe x,

Thank you for your OIA request to the Department of Internal Affairs (included with this email)

The Department will provide its response to your request as soon as practicable and within twenty working days. The 20th working day is XX

Please note that in cases where the Department's response provides information that is identified to be of general public interest, the response may also be published on the Department of Internal Affairs website. If the Department publishes its response to your OIA request, all personal information, including your name and contact details, will be removed.

Ngā mihi

Allocate OIA

Tēnā koe x,

The Department has received the below request.

Please reference OIAXX in your response, which is due to the requester by XX

Acknowledgement is attached
Acknowledgement sent by business unit

Ngā mihi

Clarify/refine request scope

Tēnā koe x,

Thank you for your OIA request to the Department of Internal Affairs (included with this email)

You have requested:

- X

To be able to assist you further with your request, we need to find out more about the particular information you are seeking.

[question]

Or

Statement about the volume of info potentially in scope, or the volume of information that would need to be searched to be able to identify the information.

The scope of your request would require the Department to undertake substantial collation and research to able to answer it, and this would be likely to disproportionately impact the normal operation of the Department. We have considered whether extending the timeframe for response or fixing a charge would enable your request to be answered, however neither option is suitable as the time needed cannot be accurately estimated. For this reason, the Department is considering refusing your request.

I am contacting you in order to give you the opportunity to refine your request to enable it to be answered without substantial collation and research.

[suggestion if applicable]

Please contact the Department as soon as possible to advise whether you would like to refine your request scope. If we do not receive response from you by XX, a decision will be made on your request, and this may result in your request being refused.

If you would like to discuss your request with us by phone, you are able to contact X at X

Ngā mihi,

Confirm clarified/refined request

Tēnā koe x,

Regarding your OIA request to the Department of Internal Affairs, discussed with you on XX, our understanding of your request is:

XX

If we have not correctly understood your request and you would like us to amend it, please let us know by responding with the corrected wording of your request.

Please note that your amended/clarified request is being treated as a new request replacing the original, in accordance with section 15(1AA) of the Official Information Act 1982. The timeframe for response changes accordingly.

The Department will provide its response to your request as soon as practicable and within twenty working days. The 20th working day is XX

Ngā mihi,

Consult with agency on transfer

Kia ora koutou x colleagues,

The Department of Internal Affairs has received the attached request and is proposing transfer of this request to your agency for response.

Transfer is in accordance with section 14(b)(i) and (ii) of the Act. The information requested is not held by the Department of Internal Affairs, but we believe it is held by, and more closely related to the functions of XX

Please confirm whether you accept transfer of this request, or advise reasons why this request should not be transferred.

If transfer is accepted, we will notify the requester of the transfer and will forward a copy of this notification to you.

I am available to discuss this transfer if helpful.

Ngā mihi,

Notify requester of transfer

Tēnā koe x,

Thank you for your OIA request to the Department of Internal Affairs (included with this email)

As the information you have requested is not held by the Department of Internal Affairs, but is believed to be held by, and more closely related to the functions of XX, we are transferring your request to that agency for response, in accordance with section 14(b) of the Official Information Act 1982.

You can expect to hear from the receiving agency shortly in regard to your request. If you would like to contact them directly, you are able to email them at the following addresses:

XX

You have the right to seek an investigation and review by the Ombudsman of this decision to transfer. Information about how to make a complaint is available at www.ombudsman.parliament.nz or Freephone 0800 802 602.

Ngā mihi,

Confirm transfer to agency

Cheers x,

I confirm this request is now transferred to XX in accordance with section 14(b) of the Act.

I attach the original request and notification of transfer sent to the requester.

You have the right to seek an investigation and review by the Ombudsman of this decision to transfer. Information about how to make a complaint is available at www.ombudsman.parliament.nz or Freephone 0800 802 602.

Ngā mihi

Notify transfer to agency without consultation

Kia ora koutou X colleagues,

The Department of Internal Affairs has received the attached request, addressed to X and is transferring this request to your agency for response.

Transfer is in accordance with section 14(b)(i) and (ii) of the Act. The information requested is not held by the Department of Internal Affairs, but we believe it is held by, and more closely related to the functions of X

I attach the original request and notification of transfer sent to the requester.

You have the right to seek an investigation and review by the Ombudsman of this decision to transfer. Information about how to make a complaint is available at www.ombudsman.parliament.nz or Freephone 0800 802 602.

Ngā mihi

Consult third party on information release

Tēnā koe X,

The Department of Internal Affairs (Department) has received a request for information under the Official Information Act 1982 which includes in its scope some information that relates to you, and which XX be released as part of the Department's response to the request.

This information includes: XX

or

I attach the information that relates to you that falls within the scope of the OIA request.

The Official Information Act 1982 requires government agencies and entities to release any official information that they hold, unless good reason exists to withhold the information under [section 6](#), [section 7](#) or [section 9](#) of the Act. It also requires that, if any reasons to withhold may exist under section 9 of the Act, the agency also consider whether there may be a greater public interest in releasing the information.

If advising

We have reviewed the information and have identified no good reason under the Act for the information to be withheld in this case.

We have reviewed the information and have identified that while a reason to withhold the information exists under section 9(2)XX of the Act, there is a strong public interest in releasing the information, in order to increase the transparency and accountability of government or to enable better public participation in the activity of government.

It is anticipated that this information will be released on XX. If you have any questions or feedback about this information release, please do not hesitate to email OIA@dia.govt.nz. If you would like to discuss this release by phone, you are also able to contact NAME at PH.

If consulting

If you have any questions about the release of the information that relates to you, or if you would like to provide feedback or information to assist the Department to make its decision regarding the release of this information, please respond by no later than XX.

If you would like to discuss this request with us by phone, you are also able to contact NAME at PH

Ngā mihi,

Extend request

Tēnā koe x,

I am contacting you to advise that the Department of Internal Affairs is extending the timeframe available for response in your request under section 15A(1)(a) of the Official Information Act 1982, as substantial collation and research is necessary to be able to answer your request.

I am contacting you to advise that the Department of Internal Affairs is extending the timeframe available for response in your request under section 15A(1)(b) of the Official Information Act 1982, as consultations necessary to make a decision on your request are such that the request is not able to be completed within twenty working days.

The response timeframe is being extended by X working days. The Department's decision on your request will be provided to you as soon as practicably and no later than XX.

Ngā mihi

Issue Decision/interim response/final response letter

Tēnā koe x,

Please refer to the attached correspondence, which provides the Department's decision on your OIA request.

Ngā mihi,

Redirect requester to make Archives research request

Tēnā koe x,

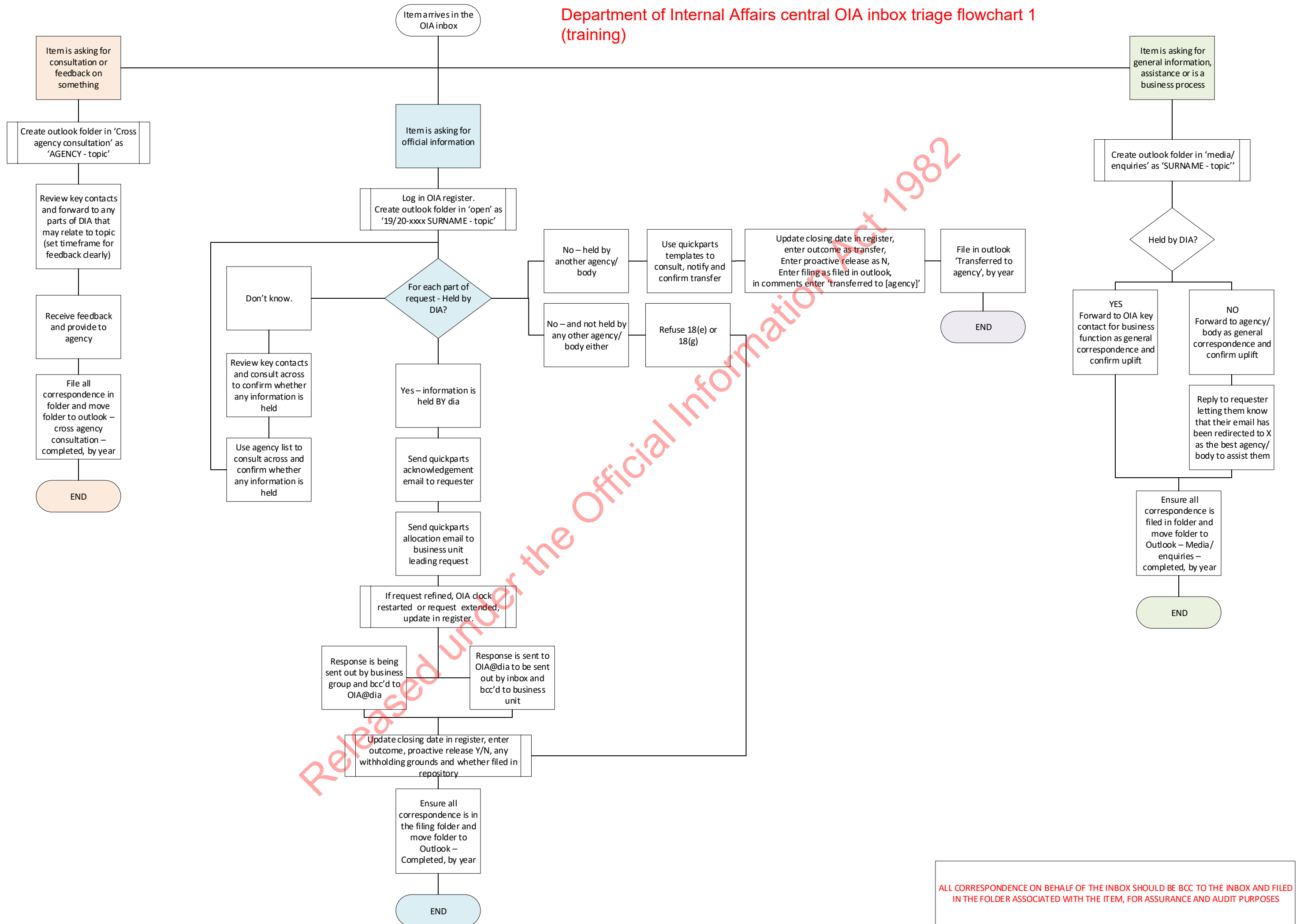
The information you have requested is more than 25 years old and is therefore likely to be held by Archives NZ. Official information that is transferred to Archives NZ, becomes part of Archives collections and access is regulated by the [Public Records Act 2005](#) rather than the Official Information Act 1982.

You are able to search Archives NZ holdings using the Archway portal: <https://www.archway.archives.govt.nz/>

If you would like an Archivist to undertake a detailed search of the Archive to assist you with your research, you are able to make a research request to Archives NZ. Please note that in some cases there may be an associated charge. You can make a research request using this webform: <https://archives.govt.nz/search-the-archive/get-help>

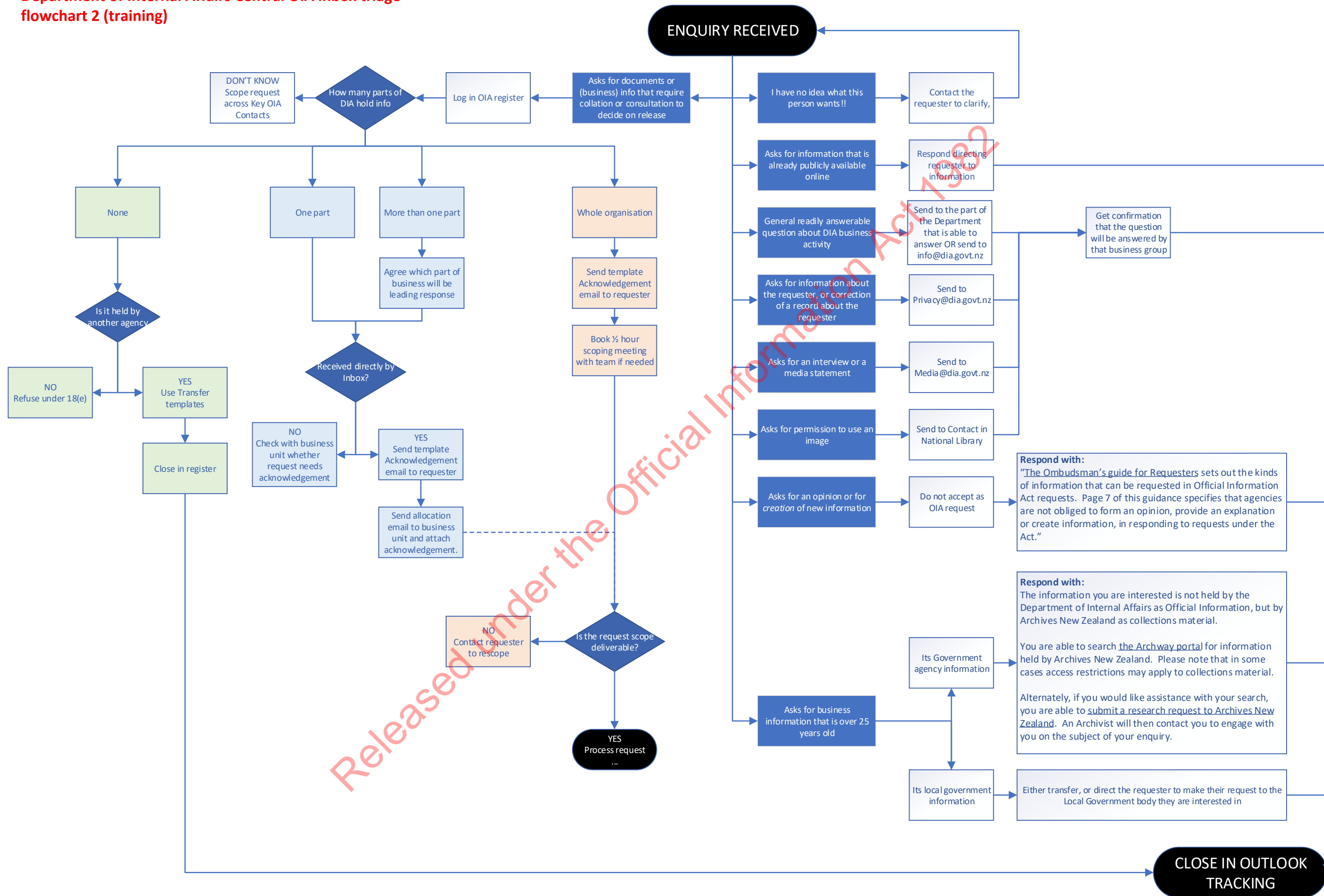
Ngā mihi

Department of Internal Affairs central OIA inbox triage flowchart 1 (training)



ALL CORRESPONDENCE ON BEHALF OF THE INBOX SHOULD BE BCC TO THE INBOX AND FILED IN THE FOLDER ASSOCIATED WITH THE ITEM, FOR ASSURANCE AND AUDIT PURPOSES

Department of Internal Affairs Central OIA inbox triage flowchart 2 (training)



Released under the Official Information Act 1982

DIA document redaction and web standards processing handout (accompanies training)

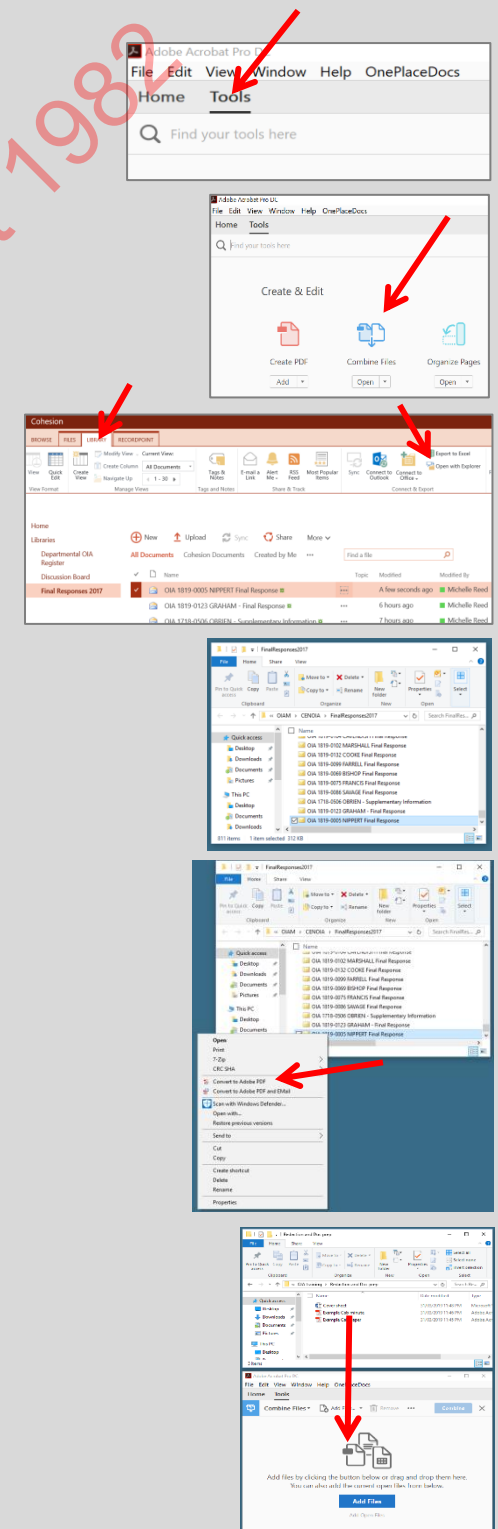


Preparing to redact in Adobe Pro DC

- Open Adobe Pro DC
- Select **'Tools'** in the upper left hand corner of the screen.
- Select **'Combine files'**
- Open your file in file explorer in cohesion. (see next section for instructions on how to do this)
- If you do not have access to file explorer in cohesionK (i.e. the icon displays as grey), you will need to save your files to your desktop and drag and drop them into Adobe from there.

Opening files in Cohesion file explorer

- Go to the location in cohesion where you have filed the documents you want to open in Adobe. In the cohesion top row menu select **'library'**. Then, in the section 4 panel titled 'Connect and Export' select **'Open with Explorer'**.
- An explorer window should now open showing the files in that file folder. You should be able to double click on PDF files to open in Adobe Pro DC, or drag and drop Word and PFD files from this window directly into Adobe pro DC.
 - If you are including outlook emails, you will need to convert this correspondence to PDF format before you are able to enter it into Adobe.
 - For a small quantity of correspondence – do this by right clicking on each email in turn in the explorer window and selecting from the dropdown menu **'Convert to Adobe PDF'**.
 - If you have a large quantity of correspondence, print all emails, order them chronologically and scan the full set to yourself (producing one PDF file).
- **Drag and drop** all PDF or word items into the Adobe pro window and rearrange them into the order you would like them to display in in the final document.



Released under the Official Information Act 1982

- Select combine files at top right hand side of window. After documents are combined into 'binder 1', save the file into your OIA request filing folder. Your name should include the label '- clean'.

Redacting in Adobe Pro DC

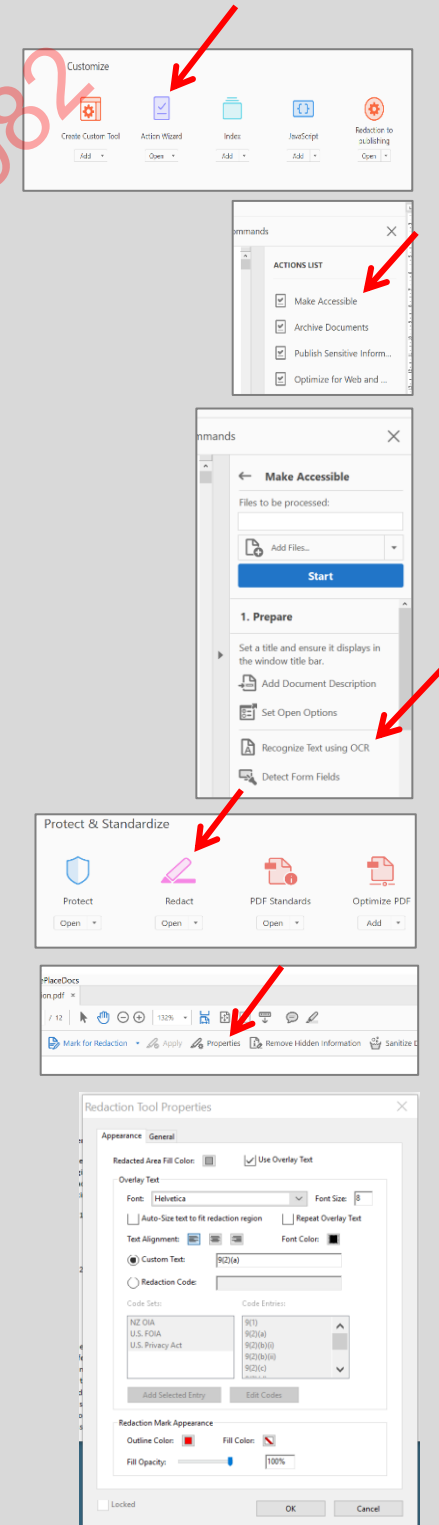
At this point you should have combined all documents you want to include into a single file and have the file open in Adobe Pro DC.

Convert your file into a text recognised format.

- Select Tools menu in the upper left hand corner of the screen.
- Scroll down the tools menu screen to the 'Customise' section and select 'Action Wizard'.
- Select 'Make Accessible' in the right hand panel menu that will appear
- Select 'Recognise Text using OCR' from the new right hand panel menu and then OK. (note there may be some errors notified during the process due to logos and images. This is fine. Ignore them and continue.)
- When the process has completed save your file.

Set the redaction appearance you want to use

- Select Tools menu in the upper left of the screen
- Scroll down the tools menu screen to the 'Protect & Standardize' section, and select 'Redact'.
- In the Redact tool's top ribbon, select 'Properties'.
- In the Redaction Tool Properties menu:
 - Ensure the 'redacted area fill colour' box is a mid-grey colour
 - Decide if you will use overlay text to annotate your redactions.
 - If you are using overlay text – ensure
 - font is Helvetica,



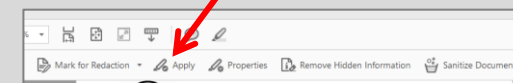
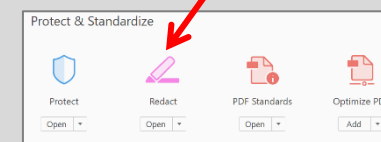
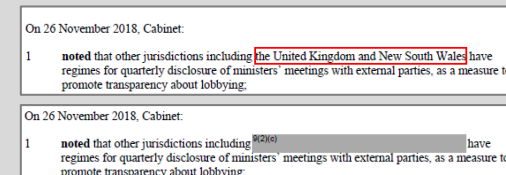
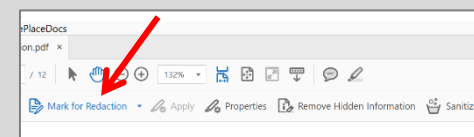
- Font size is 8,
- text alignment is left,
- font colour is black.
- Enter your custom text e.g. 9(2)(a).
Note –you will need to return to the properties menu to change the custom text to annotate a different section of the Act.
- In the bottom section ‘redaction mark appearance’ – select red as the outline colour. Fill colour should be set to ‘no colour’.
- Select ‘Ok’

Mark up your redactions in the document

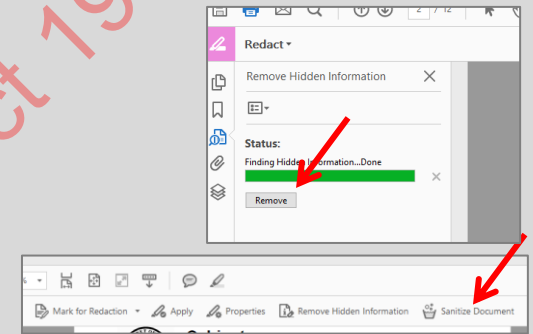
- In the Redact Tool’s top ribbon, select ‘Mark for redaction’ and then ‘Text and images’ from the pulldown options that will appear.
- Highlight over any text you want to mark for redaction.
- You will see a red box now surrounds any text you have highlighted. If you hover over this area, the final appearance of your redaction will display.
- If you find you have made a mistake and want to undo any marked text, simply click on the marked text and press delete. This will remove the redaction markup. It will not affect the text below the markup.
- When you are satisfied all information to be withheld has been marked up, save your document as a new name. You should change the filename from ‘clean’ to ‘-markup’.

Complete your redactions in the document

You have used your markup document for consultation, and now your proposed withholding has been signed off by your approver. You are ready to finalise your document.



- Select Tools menu in the upper left hand corner of the screen
- Scroll down the tools menu screen to the 'Protect & Standardize' section, and select 'Redact'.
- In the Redact tool's top ribbon, select 'Apply' and then OK.
- After the redactions have been applied, a message window will pop up and ask if you would like to search for hidden information. Select OK.
- A panel will open on the left hand side and you will see Adobe searching your file. When it has finished, select 'Remove' and OK.
- Now, in the Redact tool's top ribbon, select 'Sanitize Document' and then OK.
- Save your document as a new filename. You should change '-markup' to '-redacted'.

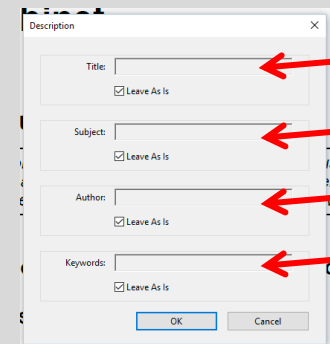
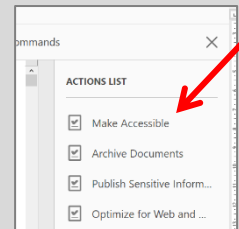
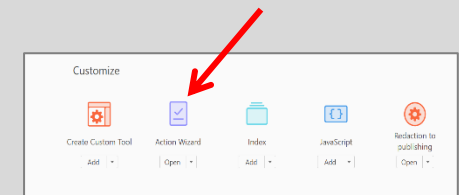


Finalising the document for release

The redacted document is in a *safe* format for release, however there are some finishing touches you must apply before you can send it out.

Make your document screen-reader accessible

- Select Tools menu in the upper left hand corner of the screen.
- Scroll down the tools menu screen to the 'Customise' section and select 'Action Wizard'.
- Select 'Make Accessible' in the right hand panel menu that will appear. You are going to go through this complete process this time.
- Select 'Start' from the new right panel menu that appears.
 - In the 'Description' window that pops up
 - The **Title** of your document will be the Cabinet reference number for Cab papers, the OIA reference number for OIAs. Never include the name of a person in this section.
 - The **Subject** of your document will be a short summary of what the document is 'about'. E.g. Change to passport fees.

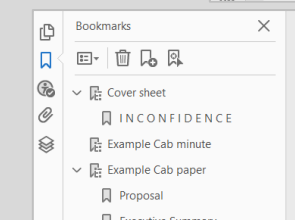
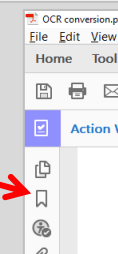
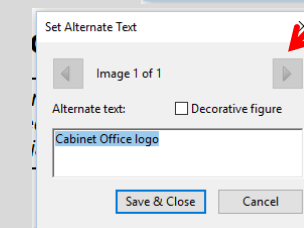
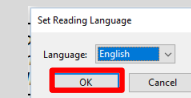
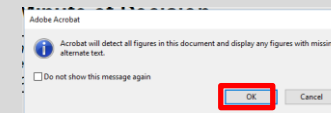
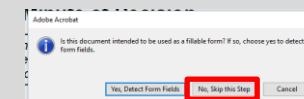
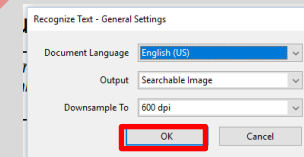


- The **Author** of your document will be 'The Department of Internal Affairs'.
- **Keywords** might include Cabinet paper, OIA, or similar, along with subject words.

- In the 'Recognise Text – General Settings' window that pops up, click OK.
- In the **fillable form** window that pops up, click No, skip this step.
- In the 'Set reading language' window that pops up, click OK.
- A message box will pop up to tell you Adobe will detect all figures in the document. Click OK.
- In the 'Set Alternate text' window that pops up, after Adobe has finished checking, you are given the option to enter text to explain what figures are.
 - You will see something like 'Image 1 of 20' and a white text field below. This is where you can enter your explanation of the figure. E.g. Cabinet Office logo.
 - Press the **arrows on left and right** to tab through your figures and enter text for them.
 - Note that Adobe will also pick up redacted areas as figures.
 - When you have entered text for all of your figures, press OK.
- The next window will ask you if you want to complete an accessibility check. This is not needed. You can click cancel.

Add bookmarks to your document

- On the left hand side of the screen halfway down the page you will see a small arrow, indicating where you can pull out the left side panel. Click this arrow.
- Select the **Bookmarks** icon. (It looks like a ribbon).
- Check that the bookmarks displayed in your document are appropriate.
 - You can remove bookmarks by clicking on them and then pressing the rubbish bin icon
 - You can add bookmarks by clicking on the place in the document that you want to bookmark and then pressing the icon that looks like a ribbon with a plus sign
 - If you double-click on any of the individual bookmarks, you can rewrite them.



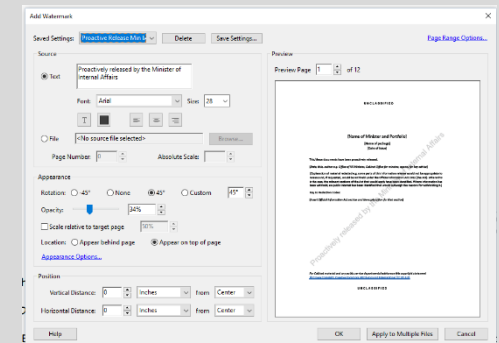
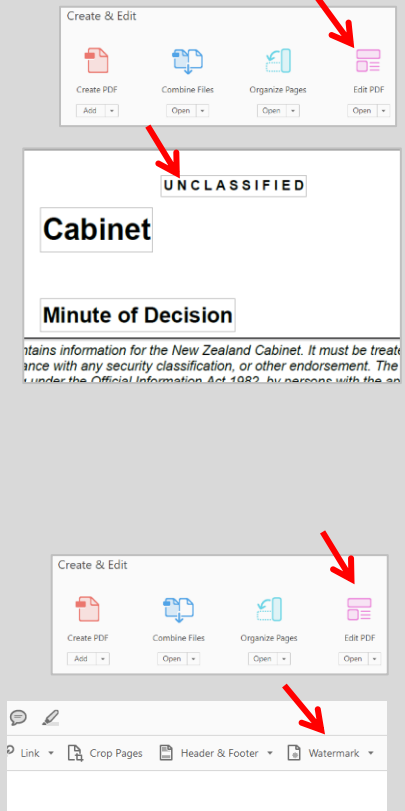
Consider changing security classifications in your document

If your document is being proactively published on the DIA website, you should change the classifications marked on the document to Unclassified.

- Select Tools menu in the upper left hand corner of the screen.
- Scroll down the tools menu screen to the 'Create and Edit' section and select 'Edit PDF'.
- Grey boxes will appear around all text sections in the document. Click on the **classification boxes** and rewrite them (each) to state UNCLASSIFIED.
- Remember to centre the text in the box.

Add a watermark to your document

- Select Tools menu in the upper left hand corner of the screen.
- Scroll down the tools menu screen to the 'Create and Edit' section and select 'Edit PDF'.
- In the Edit Tool's top ribbon, select 'Watermark', and then 'add' from the pulldown menu that appears.
- In the **Add Watermark window** that pops up:
 - In the 'source' section
 - text should read either e.g. 'Proactively released by the Minister of Internal Affairs' or 'Proactively released by the Department of Internal Affairs' or 'Released under the Official Information Act 1982'
 - Font should be Arial.
 - Size should be 36 for an A4 page

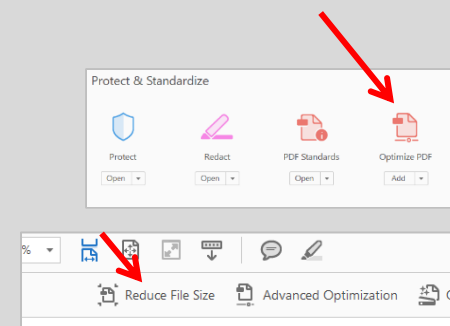


- Colour should be mid-grey for a proactive release and scarlet red for an OIA request
- Text should be centred
- In the 'appearance section'
 - Rotation should be 45 degrees
 - Opacity should be 35%
 - Text should appear on top of page.
- Depending on the document being released, if you would like to remove the watermark from the top page, you are able to do this in 'page range options' in the top right of the 'Add Watermark' window.
- Save your document. Your filename should include the label 'release copy'

Reduce the file size of your document if necessary

- Select Tools menu in the upper left hand corner of the screen.
- Scroll down the tools menu screen to the 'Protect & Standardize' section and select 'Optimize PDF'
- In the Optimise PDF top ribbon, select 'Reduce File Size' and click OK to the message box that pops up.

Be aware that reducing filesize downsamples the quality of your file. You should never downsample the same document more than once. You are able to downsample more than the standard measure suggested by Adobe, but exercise caution in doing so. The objective is to end up with a releasable file. In some cases this may mean that you need to release two files at good quality rather than one file at poor quality.





UNCLASSIFIED

Privacy policy

Date approved	4 October 2019
Review date	4 October 2020
Policy owner	Departmental Privacy Officer
Cohesion link	https://dia.cohesion.net.nz/Sites/GOV/DIAOrganisationalPolicies/_layouts/15/DocIdRedir.aspx?ID=FUJSWU7TPTWC-825107103-102

Policy overview

1. This policy describes how the Department of Internal Affairs (DIA) will ensure that our employees, partners, members of the public, and the Government retain the highest level of confidence in our ability to safeguard the personal information we hold.
2. DIA plays a privileged and trusted role as guardian of much of our nation's personal information. Because of this role, we place privacy at the core of how we work for the public. Our systems, processes, and practices provide a comprehensive and sound platform for safeguarding personal information. Our people are expected to manage the personal information we hold in a knowledgeable and respectful manner.

Audience and application

3. The audience for this policy is all DIA employees.
4. It applies to:
 - All DIA employees. For the purposes of this policy all DIA staff includes permanent, temporary and events-based staff members, as well as people contracted by or in a business relationship with DIA, including volunteers and other unpaid positions;
 - All information, regardless of medium, format or where it is stored, that has been created or received in the course of business functions, processes, decision making, actions and transactions;
 - All business activities;
 - Inter-agency initiatives where DIA is the lead agency or where it is agreed that DIA owns or is responsible for the resulting information.

International application

5. DIA provides services to, and receives support from, a global community of customers, employees, vendors, and partners. The prevalence of digital technology and online services has led to considerable consumer awareness of how personal information is managed. Many jurisdictions have sought to protect the rights of individuals by enacting laws with extra-territorial application.

6. DIA operates offices in New Zealand, Australia, and the United Kingdom. The services we offer are available online and accessible anywhere in the world.
7. Laws outside New Zealand may have application to DIA and its management of personal information. To manage the variations between the privacy protections mandated in the jurisdictions we are located in and our domestic law, DIA has adopted this policy, which applies international best practice for managing personal information and meets or exceeds legislative requirements except where noted.

Delegated authorities

8. The delegated authorities that apply are set out in the Delegations policy.

Accountability

9. The Executive Leadership Team (ELT) is accountable for this policy.

Responsibilities

10. All DIA employees are responsible for protecting personal information entrusted to DIA.
11. ELT has the responsibility for ensuring DIA has appropriate policies and processes to safeguard the personal information entrusted to us.
12. ELT are responsible for creating and nurturing a respectful privacy culture in DIA.
13. Deputy Chief Executives are responsible for assuring the Chief Executive that their Branches comply with DIA policies and processes to safeguard the personal information it holds.
14. The Departmental Privacy Officer is responsible for monitoring DIA's compliance with legislative requirements and international best practice, and for advising ELT about any risks to our ability to protect and manage the personal information we hold.

Third party engagement

15. DIA's responsibility to manage personal information extends to include third parties that DIA enters in to agreements with to share information or to supply services that involve the management of personal information on behalf of DIA.
16. DIA will ensure that any potential third-party supplier is made aware of these obligations in agreement terms and during the procurement processes, so that they can ensure they have the appropriate measures in place to meet these obligations.
17. DIA will offer contract terms which will be available for all vendors and suppliers to incorporate in to agreements to manage personal information on behalf of DIA.
18. DIA recognises many third parties will be aware of these obligations and will have developed their own contract terms to address this. DIA will evaluate any such terms when engaging in a business relationship with the third party to ensure the responsibilities of both parties are understood and agreed.

Detailed policy

Guiding principles

19. DIA's management and protection of personal information will be guided by the following principles:
 - We will embody a culture in which personal information is protected and respected;
 - Individuals can have confidence that DIA is a trusted guardian of their personal information;
 - All personal information we hold will be managed and used in accordance with international best practice and the legislative and regulatory obligations created in the jurisdictions in which we are located.
20. Our commitment to privacy will be shown by:
 - Only collecting personal information which is necessary to undertake our functions;
 - Being transparent and open about what personal information is being collected;
 - Giving individuals the opportunity to make an informed choice about the personal information they provide, or how much personal information they provide;
 - Ensuring all individuals have the right to access personal information we hold about them and the right to seek correction if that information is wrong;
 - Establishing a clear and lawful purpose for collecting personal information, and only using and disclosing personal information in accordance with that purpose;
 - Taking reasonable steps to make sure that personal information is accurate before we use it;
 - Protecting personal information from loss, misuse, and unauthorised access or disclosure;
 - Responding quickly and appropriately if a privacy breach occurs or is suspected.
21. To achieve this DIA will:
 - Implement best practice end-to-end privacy management processes. We will do this by:
 - Embedding privacy by design principles into service design so that privacy protection is at the forefront of systems and business processes.
 - Utilising privacy impact assessments in all new business process development where personal information is involved.
 - Testing and auditing our current systems to actively identify risks to privacy security and apply treatments when risks are identified.
 - Ensure our employees are confident and knowledgeable in their approach to managing personal information. We will do this by:
 - Providing resources, training and guidance material on privacy practices.
 - Using our privacy communication strategy to focus and raise awareness of privacy with our employees.
 - Regularly assess the state of our privacy health. We will do this by:
 - Measuring DIA against the [Privacy Maturity Assessment Framework](#).

- Reviewing and refreshing our privacy programme to continually lift our performance against all elements of the [Privacy Maturity Assessment Framework](#).
- Monitoring how we manage privacy requests, complaints and breach responses and implementing changes to our processes if deficiencies are identified.
- Provide effective leadership on privacy across DIA. We will do this by:
 - Empowering our Departmental Privacy Officer to undertake effective monitoring and oversight of our compliance with legislative requirements.
 - Equipping our managers with privacy skill and knowledge so they can effectively enable our staff and systems to protect individual privacy.
 - Establishing and utilising a network of privacy champions to provide guidance and support to our branches.

Definitions

22. The following definitions apply when interpreting this policy:

- **Departmental Privacy Officer** – the General Manager Information and Safety is the Department’s designated Departmental Privacy Officer under [s23 of the Privacy Act 1993](#). Their functions include:
 - Encouraging compliance with legislative requirements and international best practice.
 - Working with the Office of the Privacy Commissioner in relation to any investigations the Privacy Commissioner may be undertaking.
- **Personal information** – is any information held by the Department, in any format, which is about an identified or identifiable individual.

For the avoidance of doubt; this includes unique identifiers, location information, biometric information, and aggregate or statistical information which has not been anonymised or pseudonymised.

Legislation

23. This policy seeks to ensure DIA meets or exceeds the obligations created under the following legislation:

- [New Zealand Privacy Act 1993](#)
- [Australian Privacy Act 1988](#)
- [The General Data Protection Regulation of the European Union](#)

24. DIA recognises the potential for discrepancy in application between the above legislation, and other Acts which amend or overwrite the obligations created therein. In a scenario where DIA is unable to reconcile two competing requirements, we will prioritise the obligations under New Zealand law.

25. We note that there is likely to be such a discrepancy between the New Zealand [Public Records Act 2005](#) and [Article 17 of the General Data Protection Regulation](#).

Related documents:

26. The following documents are relevant to this policy:

- [Privacy Maturity Assessment Framework](#)
- [Delegations Policy](#)

Released under the Official Information Act 1982