Australian Government
Comcare

PRIVACY POLICY

Last review	June 2022
Next review	June 2023
Policy owner	Statutory Oversight

CONTENTS

COMCARE'S PRIVACY POLICY

Comcare takes its privacy obligations very seriously and is committed to meeting the highest standards when collecting, storing, using and disclosing personal information.

Comcare is required to comply with the *Privacy Act 1988* (Privacy Act) when handling personal information and must have a clearly expressed and up to date privacy policy. Comcare implements practices, procedures and systems relating to its functions and activities to ensure that it complies with the Australian Privacy Principles (APPs), including:

- complying with the requirements of the *Privacy Act 1988* (Privacy Act), *Privacy Amendment (Notifiable Data Breaches) Act 2017* and the *Australian Government Agencies Privacy Code*
- ensuring all Comcare staff understand and comply with Comcare's privacy obligations and this privacy policy
- responding promptly and transparently to privacy complaints
- conducting audits and quality inspections of data systems and information processes
- maintaining an effective working relationship with the Office of the Australian Information Commissioner (OAIC).

WHAT IS THE PURPOSE OF THIS PRIVACY POLICY?

The purpose of this privacy policy is to:

- clearly communicate Comcare's personal information handling practices
- enhance the transparency of Comcare's operations
- give individuals a better and more complete understanding of the sort of personal information that Comcare holds, and the way it handles that information.

The Privacy Act sets the minimum standards Comcare, as an Australian Government agency, has to meet when handling personal information.

'Personal information' is defined in the Privacy Act as:

- 'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  a) whether the information or opinion is true or not; and
  b) whether the information or opinion is recorded in a material form or not.'

The Privacy Act contains thirteen APPs which:

- set out legally binding standards for handling personal information
- regulates how Comcare can collect, store, use and disclose personal information
- requires Comcare to allow people to access the information about them that Comcare keeps
- requires Comcare, in certain circumstances, to allow people to correct or update information about them.

The APPs are contained in Schedule 1 of the Privacy Act. They can be found on the OAIC website.

Comcare may review and update this policy from time to time, to take account of new laws or technology, or changes to Comcare's functions, operations or practices.

This privacy policy is published on Comcare's website. If you would like a copy of this policy in another form, please contact Comcare's Privacy Officer using the contact details at the end of this policy.

WHAT KINDS OF PERSONAL INFORMATION DOES COMCARE COLLECT AND HOLD?

COLLECTION OF SOLICITED INFORMATION

Comcare only collects personal information if it is reasonably necessary for, or directly related to, one or more of Comcare's functions or activities. These include functions and activities under the:

- *Safety, Rehabilitation and Compensation Act 1988* (SRC Act)
- *Work Health and Safety Act 2011* (WHS Act)
- *Seafarers Rehabilitation and Compensation Act 1992* (Seafarers Act)
- *Occupational Health and Safety (Maritime Industry) Act 1993* (OHS (MI) Act)
- *Asbestos-related Claims (Management of Commonwealth Liabilities) Act 2005* (ARC Act)
- *Parliamentary Injury Compensation Scheme Instrument 2016* (the PICS Instrument)

Certain information Comcare collects is 'sensitive information' as defined in the Privacy Act. Sensitive information includes information about a person's health. In particular, information contained in workers' compensation claim records, work health and safety investigation records, asbestos-related claim records, and personnel records, may be sensitive information.

Comcare will usually only collect and hold sensitive information with your consent. However, there are certain circumstances where Comcare is permitted to collect and hold sensitive information without such consent. These circumstances are described in APP 3.4 and include, but are not limited to, where the collection:

- is required or authorised by or under law
- will prevent or lessen a serious threat to somebody's life or health, or assist in the location
- of a missing person
- is reasonably necessary to allow Comcare to take appropriate action when it suspects unlawful activity or misconduct of a serious nature that relates to Comcare's functions or activities
- is reasonably necessary to establish, exercise or defend a legal or equitable claim, or for the purposes of a confidential alternative dispute resolution process
- is reasonably necessary for enforcement related activities, where Comcare is acting as an enforcement body.

COLLECTION OF UNSOLICITED INFORMATION

Comcare is occasionally provided with personal information which it has not requested or solicited. Where unsolicited information is received by Comcare, within a reasonable period, Comcare will determine whether that information is reasonably necessary for, or directly related to, one or more of our functions or activities. If the unsolicited information does not relate to one or more of

Comcare's functions or activities, subject to the requirements of the Archives Act 1983 (the Archives Act), Comcare will destroy or de-identify the information as soon as is practicable.

HOW DOES COMCARE COLLECT AND HOLD PERSONAL INFORMATION?

Collection of personal information

Comcare only collects personal information by lawful and fair means. Collection of personal information by Comcare may occur when:

- a worker's compensation claim is lodged with Comcare under the SRC Act
- Comcare seeks information, from people such as a treating health professional, in connection with assessing a worker's compensation claim
- Comcare, in its support role to the Safety, Rehabilitation and Compensation Commission (SRCC), receives information about workers' compensation claims made by employees of self-insured licensees
- Comcare receives information, pursuant to the WHS Act, relating to a workplace incident or other risk to health and safety at a workplace
- Comcare monitors or enforces compliance with the WHS Act
- Comcare receives allegations or complaints from workers or members of the public via the WHS Help Desk
- an individual lodges a common law claim against the Commonwealth, or a Commonwealth authority, for which liability has been assumed by Comcare under the ARC Act
- a worker's compensation claim is lodged with the Seafarers Safety, Rehabilitation and Compensation Authority (Seacare Authority) under the Seafarers Act
- a worker's compensation claim is lodged with Comcare under the PICS Instrument
- an individual provides information to Comcare, or its agents, in connection with a job application or employment with Comcare
- contractors or suppliers are working with Comcare
- individuals contact Comcare.

Where reasonable and practical, Comcare collects information about you directly from you. However, Comcare may also collect personal information from someone other than you with your express consent, or if it is required or authorised to do so by or under an Australian law or a court or tribunal order.

At or before the time Comcare collects information about you, or as soon as practicable after collection, Comcare will take reasonable steps to notify you or otherwise ensure that you are aware of the matters that are required by APP 5, including, but not limited to:

- the fact that Comcare has collected the information and the circumstances of the collection
- the details of the relevant law under which the collection is required or authorised (if any)
- the main consequences (if any) for you if Comcare does not collect the personal information
- how you can access and correct information about you, or make a complaint about a breach of the APPs.

Comcare may provide this notification by including privacy notices on our paper-based and online forms.

HOLDING OF PERSONAL INFORMATION

Comcare holds all its records in accordance with the provisions of the Archives Act and relevant records authorities.

Comcare takes all reasonable steps to protect the personal information that we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. This includes appropriate measures to protect electronic materials, and materials stored and generated in hard copy, and ensuring that contracted service providers are subject to the same strict privacy obligations that Comcare operates under.

Comcare's networks and websites have security features in place to protect the information that the Comcare holds from misuse, interference and loss from unauthorised access, modification or disclosure.

Audits and quality inspections are also conducted from time to time to ensure the accuracy and integrity of information, and that any systemic data quality issues are identified and resolved promptly.

STORAGE AND DATA SECURITY

Electronic and paper records containing personal information are protected in accordance with Australian Government security policies including the Attorney General's Department's Protective Security Policy Framework and the Australian Signals Directorate's Information Security Manual.

Comcare's networks and websites have security features in place to protect the information that the Comcare holds from misuse, interference and loss from unauthorised access, modification or disclosure.

DESTRUCTION AND DE-IDENTIFICATION OF PERSONAL INFORMATION

Personal information that Comcare collects and holds is usually either contained in a Commonwealth record (as defined in the Archives Act) or required to be retained by or under an Australian law. Comcare manages its records (including those that contain personal information) in accordance with the:

- Archives Act
- Administrative Functions Disposal Authority
- Commission Management, Safety, Rehabilitation and Compensation Regulation Records Authority (2015/00245318)
- Work Health and Safety Prevention, Education and Promotion; Work Health and Safety Regulation Records Authority (2013/00241702)
- Asbestos related compensation claims; Workers' compensation claim management Records Authority (2010/00322036)
- any other relevant records disposal authority.

INFORMATION HELD BY CONTRACTED SERVICE PROVIDERS

Comcare takes contractual measures to ensure that contracted service providers comply with the same privacy requirements applicable to Comcare.

WHAT ARE THE PURPOSES FOR WHICH COMCARE COLLECTS, HOLDS, USES AND DISCLOSES PERSONAL INFORMATION?

Comcare performs functions and exercises powers in connection with:

- securing the health and safety of workers and other persons at workplaces under the WHS Act
- the provision of workers' compensation and rehabilitation under the SRC Act
- the provision of workers' compensation and rehabilitation under the PICS Instrument
- the management of the Commonwealth's asbestos-related liabilities under the ARC Act
- assisting the Seacare Authority to perform its functions and exercise its powers under the OHS (MI) Act, and rehabilitation and compensation arrangements for seafarers under the Seafarers Act
- assisting the SRCC to perform its functions and exercise powers, including the granting and regulation of self-insured licensees under the SRC Act
- employment under the Australian *Public Service Act 1999*.

Comcare may collect, hold, use and disclose personal information for the purposes of these functions and exercising these powers. This includes disclosing personal information to third parties who assist Comcare in performing these functions and exercising these powers.

Importantly, exercising Comcare's functions and powers necessitates processes that support ICT products and services which require ICT testing to ensure their security and useability. Comcare may use personal information for ICT testing. However, when dealing with personal information in an ICT testing context, Comcare will usually de-identify that information so that the information can no longer be used to identify you. If personal information is not de-identified, Comcare will deal with personal information collected during ICT testing only where you would reasonably expect this or have consented and strictly in accordance with the Privacy Act.

Where Comcare holds information about you that was collected for a primary purpose (such as administering a workers' compensation claim), it does not require your consent to use and disclose the information for that purpose. However, Comcare will not use or disclose the information for another purpose (a secondary purpose) unless:

- you have consented to the use or disclosure of the information, or
- the use or disclosure falls within one of the specific exceptions in APP 6.2. This may occur, for example, where the use or disclosure:
  - is related to the primary purpose of collection, and you would reasonably expect Comcare to use or disclose the information for this secondary purpose
  - is required or authorised by or under Australian law or a court or tribunal order
  - will prevent or lessen a serious threat to somebody's life or health, or assist in the location of a missing person
  - is reasonably necessary to allow Comcare to take appropriate action when it suspects unlawful activity or misconduct of a serious nature that relates to Comcare's functions or activities
  - is reasonably necessary for establishing, exercising or defending a legal or equitable claim
  - is reasonably necessary for the purposes of a confidential alternative dispute resolution process
  - is reasonably necessary for an enforcement related activity conducted by an enforcement body.

Comcare may use personal information to improve the effective management of Comcare's business and the efficient management of claims. This may include Comcare or its contractors using personal information to conduct research, policy development and for internal administrative purposes. Where feasible, the information will be de-identified. De-identified [personal] information may also be used for research, data analysis and educational purposes.

If Comcare notifies you that personal information about you may be used or disclosed for a related secondary purpose, Comcare will consider that you would 'reasonably expect' that your personal information would be used or disclosed for that secondary purpose. Please contact the Privacy Officer if you have any concerns about such uses or disclosures of information about you.

WHAT ARE THE MAIN CONSEQUENCES FOR YOU IF COMCARE DOES NOT COLLECT YOUR PERSONAL INFORMATION?

If Comcare does not collect personal information from you for the purposes of performing one of its functions it may impact the performance of that function.

CLAIMS MANAGEMENT

If you make a claim for compensation under the SRC Act and choose not to provide Comcare with personal information required for your claim, or your express written consent for Comcare to use and/or disclose your personal information to manage your claim, Comcare may not process your claim until you provide the requested information or consent.

If you make a claim for compensation under the SRC Act and do not provide consent for Comcare to collect personal information from your treatment providers, Comcare may exercise its power to require you to undergo a medical examination.

In some instances, your claim may be managed by a contracted service provider under delegated claims services arrangements. You are not able to veto these delegations.

If you do not want information about you to be collected, used or disclosed for managing your claim, you may withdraw your claim.

WORK HEALTH AND SAFETY

If you fail to comply with compulsory requests for information under the WHS Act, a statutory penalty may apply. Comcare does not need consent to use or disclose compulsorily acquired personal information when it is being used or disclosed for the primary purpose of collection.

COMCARE (AS AN EMPLOYER)

If you do not provide relevant personal information in an application for employment with Comcare, Comcare may not be able to process your application.

HOW CAN YOU ACCESS AND CORRECT PERSONAL INFORMATION THAT COMCARE HOLDS?

Comcare takes all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, up-to-date and complete.

You can request access at any time to the information about you Comcare holds. You may also ask Comcare to either correct the information or include a statement indicating that the information is inaccurate, out of date, incomplete, irrelevant or misleading. To do so, please contact the Privacy Officer.

Comcare will respond to requests for access or correction within 30 days. No charges apply to requests for access to, or correction of, information about you.

You can also request any document held by Comcare that relates to your worker's compensation claim under section 59 of the SRC Act.

Comcare can decline access to, or correction of, personal information under circumstances set out in the Privacy Act. Where access is refused, Comcare will give you written notice of the reasons for refusal and the mechanisms available to you to dispute that decision.

WILL COMCARE USE PERSONAL INFORMATION FOR DIRECT MARKETING?

When Comcare undertakes commercial activities, these are subject to the same restrictions on using or disclosing personal information for direct marketing purposes that apply to private sector organisations.

Comcare does not typically use or disclose personal information for direct marketing purposes in connection with our commercial activities. Comcare will only use or disclose personal information for direct marketing purposes, where this is permissible under APP 7. For example, we:

> obtain your consent to use or disclose information about you for direct marketing purposes if it is practicable, unless you would reasonably expect Comcare to use or disclose the information for direct marketing purposes

> provide a simple means by which you may easily request not to receive direct marketing communications from Comcare

WILL COMCARE SEND PERSONAL INFORMATION OVERSEAS?

Comcare is unlikely to disclose personal information to a person who is not in Australia or an external Territory. However, there are instances in which this may occur. For example:

> if a person has been located outside Australia or an external Territory and is seeking, or has sought, medical attention or undergone rehabilitation activities in relation to a claim

> where Comcare is investigating a WHS incident that occurred overseas or involved witnesses who are located overseas

> where Comcare is assessing a worker's compensation claim which involved witnesses who are located overseas

Whenever disclosing personal information to an overseas recipient, Comcare will comply with APP 8.

If you nominate an email account to communicate with Comcare, you acknowledge your email service provider may store information in data centres outside of Australia. By providing Comcare with permission to email information to your nominated address you are consenting to this possibility.

CAN YOU DEAL WITH COMCARE ANONYMOUSLY?

Your identity is typically relevant to the fulfilment of Comcare's purpose for collecting, using, holding or disclosing personal information. Most of the time, it is not likely to be practicable for Comcare to deal with you, such as when managing a compensation claim, if you have not identified yourself or have used a pseudonym.

However, in other circumstances, individuals can remain anonymous or use a pseudonym when interacting with Comcare, including when reporting or discussing concerns about suspected fraud relating to workers' compensation claims, or risks to health and safety at a workplace.

If you are concerned about not being able to deal with us anonymously, you can make an anonymous inquiry by contacting the Privacy Officer and explaining the circumstances.

HOW CAN YOU MAKE A COMPLAINT ABOUT A BREACH OF THE AUSTRALIAN PRIVACY PRINCIPLES?

You may make a privacy complaint if you consider that Comcare has interfered with your privacy or otherwise breached its obligations under the APPs in relation to the management of information about you.

Any complaints should be in writing, providing as much detail as possible, and addressed to the Privacy Officer by emailing privacy@comcare.gov.au.

Comcare will take reasonable steps to investigate any complaint, and to notify you of the outcome of our investigation within 30 days.

If we do not respond to the complaint within 30 days, or you are not satisfied with the outcome of Comcare's privacy assessment, you can make a complaint directly to the Office of the Australian Information Commissioner. Further details about how to make a complaint are set out at on the OAIC website.

HOW CAN YOU CONTACT COMCARE'S PRIVACY OFFICER?

The Privacy Officer can be contacted by:

Telephone	1300 366 979
E-mail	privacy@comcare.gov.au
Post	Privacy Officer Comcare GPO Box 990 CANBERRA ACT 2601

If you require interpreter services, details of how to access these services are available on Comcare's website.

Australian Government

Comcare

PRIVACY MANUAL AND PROCEDURES

Contents

Comcare's Privacy Obligations

As an Australian Government Agency, Comcare is required to comply with the requirements of all relevant Commonwealth privacy legislation and regulations, including the *Privacy Act 1988* (Privacy Act), *Privacy (Regulations) 2013,* and the Australian Government Agencies Privacy Code.

Privacy Act

The Privacy Act sets the minimum standards Comcare, as an Australian Government agency, has to meet when handling personal information.

The Privacy Act contains thirteen Australian Privacy Principles (APP) which:

- set out legally binding standards for handling personal information
- regulates how Comcare can collect, store, use and disclose personal information
- requires Comcare to allow people to access the information about them that Comcare keeps
- requires Comcare, in certain circumstances, to allow people to correct or update information about them.

What is Personal Information?

'Personal information' is defined in the Privacy Act as:

> *'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> > *a) whether the information or opinion is true or not; and*
> >
> > *b) whether the information or opinion is recorded in a material form or not.'*

Common examples of personal information are in an individual's name, address, telephone number, date of birth, email address medical records, bank account details, employment details and commentary or opinion about a person.

What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances.

Australian Privacy Principles

APP1: Management of Personal information

APP 1 requires that APP entities take reasonable steps to implement practices, procedures and systems to ensure they comply with the APPs. APP 1 also requires every APP entity to have a clear policy about the entity's management of personal information that addresses a list of prescribed matters. The policy must be made available free of charge and in an appropriate form (e.g. by publishing on the entity's website). Prescribed matters include:

- the kinds of personal information that the entity collects and holds;
- how the entity collects and holds personal information;
- the purposes for which the information is collected, held, used and disclosed;
- how an individual may access and, if necessary, correct the information;
- how an individual can complain about the entity's use of the information; and
- whether the entity is likely to disclose the information to overseas recipients, and if so, the countries in which such recipients are likely to be located

APP2: Anonymity and Pseudonymity

APP 2 states that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity. However, this requirement does not apply where it is impracticable for an APP entity to deal with individuals who have not identified themselves, or where the APP entity is permitted by law to deal with individuals who have identified themselves.

There are a number of instances where it is impractical for Comcare to do this. It is reasonable for someone to remain anonymous or use a pseudonym when enquiring about their obligations as a PCBU under the Work Health and Safety Act 2011 (WHS Act) or when making an anonymous tip-off. It is not reasonable for someone to remain anonymous or use a pseudonym when lodging a claim or providing a witness statement.

APP3: Collecting personal and sensitive information

APP 3 states that an APP entity must only collect personal information by lawful and fair means, and must (where reasonable and practicable) collect personal information about an individual directly from that individual.

Further, an APP entity must not collect personal information unless the information is reasonably necessary for one or more of the APP entity's functions or activities.

In addition, "sensitive information" may generally only be collected if the individual about whom the information relates has consented to the collection.

"Sensitive information" is information about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation or practices; criminal record; personal health information; genetic background, or biometric identification**.**

APP4: Unsolicited information & Commonwealth Records

APP 4 states that if an APP entity receives personal information that it has not solicited from an individual, it must first determine whether or not it could have collected the information under APP 3 if it had solicited the information. If not, the entity must destroy or de-identify the information.

Unsolicited personal information is personal information received by Comcare where we have taken no active steps to collect the information.

APP5: Notification of the Collection personal information

APP 5 requires that, when an entity collects personal information about an individual, it must take reasonable steps to notify the individual or otherwise ensure they are aware of certain matters, including:

- the organisation's identity and contact details;
- the fact that the entity has collected the information;
- any law that requires the information to be collected;
- the purposes for which the information is collected;
- the consequences for the person if the information is not collected;
- the organisations to which the information is usually disclosed;
- how the individual can access and, if necessary, correct the information;
- how the individual can complain about the entity's use of the information; and
- whether the entity is likely to disclose the information to overseas recipients and, if practicable, the countries where they are located.

Often, entities will notify individuals about the above by providing a privacy notice at the time of collection, such as on a form used to collect personal information, or in a script read over the telephone.

APP6: Using and disclosing personal information

APP 6 regulates an entity's use and disclosure of personal information. APP 6 states that an entity should only use (or disclose) personal information for the purpose for which it was collected.

An entity can use or disclose personal information about an individual for another purpose if:

- the individual consents; or
- the individual would reasonably expect the organisation to use or disclose the information for a secondary purpose, and the secondary purpose is related to the primary purpose (or *directly* related in the case of sensitive information).

An example of a related secondary purpose is where an entity collects personal information to provide a service and uses that information to evaluate or improve that particular service. An example of an unrelated secondary purpose may include where Comcare collects personal information for compensation claims processing and then discloses the same information to a third-party research company without authority.

An entity may also be able to disclose personal information for some secondary purposes related to the public interest (e.g. law enforcement, public safety, research purposes and emergency situations).

APP7: Direct Marketing

APP 7 concerns the circumstances in which an entity can use personal information for direct marketing. The term "direct marketing" is not defined in the PA 1988; however, the Explanatory Memorandum to the Act states that it involves "communicating directly with a consumer to promote the sale of goods and services to the consumer". The APP guidelines state that direct

marketing can be through "a variety of channels, including telephone, SMS, mail, email and online advertising".

APP 7 generally applies only to private sector organisations; however, it can apply to the Australian Government agencies named in schedule 2 of the *Freedom of Information Act 1982* (Cth) (FOI Act) and its regulations.

Comcare is not a named agency in Schedule 2 of the FOI Act.

APP8: Disclosing information overseas

APP 8 covers the disclosure of personal information outside of Australia. It is particularly relevant in today's context where an increasing number of entities use information technology services that disclose or transfer personal information to overseas recipients (e.g. outsourcing, off-shoring and cloud computing).

Subject to certain exceptions, before an APP entity makes personal information available to a third party located outside of Australia, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs.

This does not apply when it is the person themselves who have given us, for example, a Gmail email address to send their information to, even though Gmail stores email overseas.

APP9: Government-related identifiers

APP 9 limits the use of government-related identifiers (e.g. passport, Medicare, and drivers' licence numbers).

The purpose of APP 9 is to ensure that government-related identifiers do not become universal identifiers, and to prevent government-related identifiers from being used for data-matching. As such, APP 9 generally prohibits an entity from adopting government-related identifiers as its own way to identify an individual.

There are exceptions where using the identifier is reasonably necessary for certain purposes, such as verifying the identity of an individual.

APP10: Quality of personal information

APP 10 requires APP entities to take reasonable steps to ensure that the personal information they collect, use and disclose is accurate, up-to-date and complete. The reasonable steps required depend on the sensitivity of the information.

An APP entity is expected to take reasonable steps to ensure the quality of personal information at the time the information is collected and when it is used or disclosed.

Reasonable steps that an entity will take will depend upon the circumstances that include:

- The sensitivity of the information.
- The nature of the entity holding the information.
- The possible adverse consequences for an individual if the quality of the information is not guaranteed.
- The practicability (time and cost)

APP 11: Security of Personal Information

APP 11 concerns the security of personal information held by APP entities. It requires APP entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss and from unauthorised access, modification and disclosure. Further, the entity must take reasonable steps to destroy or de-identify the information if it no longer needs it.

APP12: Access to information

APP 12 states that an APP entity must, upon request, give an individual access to any personal information that the entity holds about them. An entity "holds" personal information if it has possession or control over it. The information does not have to be in the physical possession of the entity (e.g. where it has outsourced storage of the information but retains control over it).

All APP entities must allow individuals to *request* access to their personal information for free.

APP 12 sets time periods within which entities must respond to requests for access. Australian Government agencies must respond to requests within 30 days of the request.

There are several exceptions to APP 12 that permit an entity to refuse access to personal information. As a commonwealth agency, Comcare has the ability to refuse access to personal information under the Privacy Act if the information falls within an exemption under the FOI Act.

Comcare is obliged, under APP12 to provide reasons for any refusal, and an individual is entitled to complain to the Privacy Commissioner.

APP 13: Correcting personal information

APP13 requires an APP entity to take reasonable steps to correct any personal information it holds if it is satisfied that the information is out of date, inaccurate, incomplete, irrelevant or misleading, or if an individual requests the information to be corrected. On request from the individual, the entity must also communicate the correction to third parties to whom it has previously disclosed the information.

If an entity refuses to correct the information, it must explain (in writing) the refusal and how the individual can complain about this refusal. The entity may also have to inform users of the information that the individual believes to be incorrect.

For government agencies, APP 13 operates alongside the right to amend or annotate personal information under part V of the FoI Act (Cth).

Notifiable Data Breach Scheme

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Scheme) regulates the reporting and notification of eligible data breaches to the Office of the Information Commissioner (OAIC) and impacted individuals.

The NDB Scheme requires notification of eligible data breaches. An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

2. this is likely to result in serious harm to one or more individuals, and

3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

The NDB scheme is designed so that only serious ('eligible') data breaches are notified. If an entity is aware of reasonable grounds to *believe that there has been* an eligible data breach, it must promptly notify individuals at risk of serious harm and the Commissioner about the eligible data breach.

Deciding whether an eligible data breach has occurred involves deciding whether, from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

Comcare must take all reasonable steps to complete the assessment within 30 calendar days after the day we become aware of the grounds that caused the suspected eligible data breach.

There is an expectation that wherever possible we treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

Where an entity cannot reasonably complete an assessment within 30 days, the Commissioner recommends that it should document this, so that it is able demonstrate:

- that all reasonable steps have been taken to complete the assessment within 30 days
- the reasons for the delay
- that the assessment was reasonable and expeditious

The Office of the Australian Information Commissioner (OAIC) suggests an assessment could be a three-stage process:

Initiate: decide whether an assessment is necessary and identify which person will be responsible for completing it.

Investigate: quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts.

Evaluate: make a decision, based on the investigation, about whether the identified breach is an eligible data breach.

At any time, including during an assessment, an entity can, and should, take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. If remedial action is successful in preventing serious harm to affected individuals, notification is not required.

Procedures for assessing and identifying 'eligible' data breaches are included under the Privacy Incident procedures section of this manual.

Australian Government Agencies Privacy Code

The Australian Government Agencies Privacy Code (the Code) sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2

(APP1.2). The code requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian.

The Code requires agencies to:

- have a privacy management plan
- appoint a Privacy Officer, or Privacy Officers, and ensure that particular Privacy Officer functions are undertaken
- appoint a senior official as a Privacy Champion to provide cultural leadership and promote the value of personal information, and ensure that the Privacy Champion functions are undertaken
- undertake a written Privacy Impact Assessment (PIA) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information
- keep a register of all PIAs conducted and publish this register, or a version of the register, on their websites
- take steps to enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information

Agencies will still need to take other steps under APP 1.2 to ensure compliance with all the APP.

Comcare's Privacy Management Plan is at Annexure I

Comcare's Privacy Policy outlines our personal information handling practices, provides transparency about our operations, and gives individuals a better understanding of the personal information we hold including the way we handle that information. It also explains how an individual can gain access to or seek correction of personal information or make a complaint to Comcare if they believe a breach of the Privacy Act has occurred. See Annexure II

Privacy incidents

Overview

A privacy incident is an event notified to statutory Oversight by a Comcare or delegated claims staff member that involves an interference of privacy or potential interference with privacy. A privacy incident would typically involve an occurrence that is not in line with the APP's.

A privacy Incident It is notified internally to the Statutory Oversight team by:

- Phone (then referred to submit privacy incident report form)
- Emailing a privacy incident report form to privacy@comcare.gov.au

The Privacy incident report form captures relevant information about the incident from the staff member reporting the matter to enable the Statutory Oversight team is available on the Privacy page of Comnet. See form at Annexure III.

Each privacy incident is considered against the criteria for an eligible data breach. If it is found that there is a likelihood of serious harm, the incident should be raised with Statutory Oversight AD's who will determine if notification to the OAIC and the individual whose information was involved is warranted.

Privacy incident reports are completed within 30 days of notification. Where an interference with privacy is found, it is reported to the Team Leader and Director of the staff member responsible for the inference. The Director is provided with a copy of the incident report and advised of any recommended actions to be carried out to mitigate the risk of a recurrence. Where no interference is found only the person advising the incident is notified.

Privacy Incident Procedure

All internally notified privacy incidents are managed using the process outlined below and considering the following four key steps:

- Conduct preliminary assessment and contain
- Evaluate the risk associated with the incident
- Consideration of Notifiable Data Breach criteria
- Prevention/recommendations

Notification of incident

1. The Privacy incident report form is received through privacy@comcare.gov.au. Staff notifying incidents over the phone will be asked to submit a privacy incident report form. Form at Annexure III.
2. The Statutory Oversight Director will assign privacy incident matters to Statutory Oversight Officers.
3. Assigned officers are required to create a matter file in Trim.
    - Files are to be created under the Incident Mega Folder (MF) within SC15/89
    - Register the matter in the corresponding Privacy Matter register (financial year) located in Trim file 2014/593.
    - All correspondence is to be saved to file.

File creation process is outlined at Annexure IV.

Preliminary Assessment - Containing the incident and evaluating the risk

The reporting officer should provide enough information within the first two pages of the privacy incident report form to allow the preliminary assessment to occur. This information includes:

- A full description of the incident including
- Reporting officers name, position and team

- Time, Date and Location of the incident
- How the incident occurred – post, email, in person etc
- Description of the incident
- Claim number and Trim references (if applicable)
- Cause of the incident
- Mitigation /Action taken

If it is not clear what or how an incident has occurred contact the reporting officer and seek clarification/further information. When obtaining further information, Statutory Oversight officers must take care not to collect information beyond that which is required to assess and respond to the privacy incident.

All emails regarding privacy matters need to be sent from the Privacy mailbox. Allow up to two days for response.

The following steps should then occur:

1. Does the incident involve personal information?

   Personal information is defined as:

   Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

   a. *whether the information or opinion is true or not; and*

   b. *whether the information or opinion is recorded in a material form or not.'*

If the incident does not involve personal information, no further privacy assessment is required. It may however require further assessment by other teams (Media, Technology etc) depending on the incident. Email the notifying staff member advising no further action will be taken in regard to Privacy and inform them of any other steps or referrals made to other teams. If the incident does involve personal information continue to next step.

2. What steps have been taken to contain the incident?

Action must be taken immediately to contain the incident. If there is no indication of steps having been taken by the reporting officer, the assigned officer must request action be taken.

Email the staff member involved/reporting officer and request they take reasonable steps to contain the incident provide two days to respond to email.

Steps to contain an incident can include:

- Requesting deletion/destruction of information
- Stopping the unauthorised practice

- Recovery of records
- Shut down the system that was breached

The assigned officer should record steps taken within the incident notification form and save correspondence confirming steps taken to file.

3. Which APP's apply?

Assigned officers should apply their knowledge of the APP's to the incident to identify which APP applies. The officer should systematically consider whether each of the APPs apply. However, APPs that are not relevant to the specific matter do not need to be included in the privacy incident response.

An Officer should refer to the APP guidelines when assessing and identifying which APP is applicable:

- Openness/transparency of privacy policy and procedures (APP 1).
- Anonymity and pseudonymity (APP 2).
  - e.g. Not allowing an individual to use a pseudonym where it would be considered reasonable
- Collection of solicited or unsolicited personal information (APP 3 & 4).
  - e.g. Soliciting and collecting personal information that is not reasonably necessary to our functions or activities
  - e.g. Collection of unsolicited information without determining if it could have been collected under APP3
- Sensitive personal information (APP 3).
  - e.g. Collection of sensitive personal information without consent
- Use or disclosure of personal information (APP 6).
  - e.g. Using the personal information collected for a primary purpose for a secondary purpose without consent.
- Cross border disclosure of personal information (APP 8).
  - e.g. Sending information to an overseas person without consent
- Adoption, use or disclosure of government related identifiers (APP 9).
- Quality of personal information (APP 10).
  - e.g. emailing personal information to an old email address after having received a new updated address
- Security of personal information (APP 11).
  - e.g. Emailing personal information to an incorrect recipient

        - e.g. Losing personal information in public (on a train etc)
        - e.g. Mailing personal information to an incorrect address
    - Access to personal information (APP 12).
        - e.g. Refusing access without explanation
    - Correction of personal information (APP 13).

Most internal incidents reported to Statutory oversight involve APP11 - security of personal information. (i.e. emails to incorrect external recipients)

4. Select relevant APP on page four of the privacy incident report form and enter reasons why it applies.

When undertaking an assessment of whether there has been an interference with privacy, Statutory Oversight officers should rely on original source documents, rather than the content reported in the Privacy Incident Report form.

Evaluating the risk

When evaluating the risks associated with the incident consider the following:

- How many individuals could potentially be affected?
- Who is the recipient of the information?
- The type and amount of personal information involved
- The context of the affected information
- The cause and extent of the incident
- The risk of serious harm to an individual
    - Identity theft
    - Financial loss
    - Threat to physical safety
    - Threat to emotional wellbeing
- The risk of other harms:
    - Loss of trust and reputational damage for Comcare
    - Loss of assets

5. Details of any significant risks should be entered onto the form and discussed with AD or Director of Statutory Oversight team.

6. A risk rating based on the table below and within the privacy incident form below should be entered into the Privacy incident report

		Consequence				
Likelihood		**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Expected in most circumstances	**Almost certain**	Medium	High	Very high	Very high	Very high
Will probably occur in most circumstances	**Likely**	Medium	Medium	High	Very high	Very high
Could occur at same time	**Possible**	Low	Medium	Medium	High	Very high
Not expected to occur	**Unlikely**	Low	Low	Medium	Medium	High
Exceptional circumstances only	**Rare**	Low	Low	Low	Medium	Medium

Assessing for 'eligible data breach' under the NDB Scheme

7. When undertaking an assessment of whether the disclosure amounts to an 'eligible data breach', Statutory Oversight officers should rely on original source documents, rather than the content reported in the Privacy Incident Report form.

8. The risk rating should indicate if there are reasonable grounds to suspect that there may have been a serious breach and whether further assessment under the NDB scheme is warranted.

An eligible data breach arises when the following three criteria are satisfied:

- There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
- It is likely to result in serious harm to one or more individuals (see Is Serious Harm Likely?), and
- the entity has not been able to prevent the likely risk of serious harm with remedial action

The first step in deciding whether an eligible data breach has occurred involves considering whether there has been a data breach; that is:

- unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information.

The Privacy Act does not define these terms. The following analysis and examples draw on the ordinary meaning of these words.

Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Examples of unauthorised access include:

- an employee browsing sensitive customer records without any legitimate purpose
- a computer network being compromised by an external attacker resulting in personal information being accessed without authority

Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

Examples of unauthorised disclosure include:

- an employee of an entity accidentally publishing a confidential data file containing the personal information of one or more individuals on the internet would be considered unauthorised disclosure.
- Loss refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

The second step in deciding whether an eligible data breach has occurred involves deciding whether, from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

For the NDB scheme a ‘reasonable person’ means a person in the entity’s position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. In general, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.

The phrase ‘likely to occur’ means the risk of serious harm to an individual is more probable than not (rather than possible).

Serious harm’ is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

When assessing for serious harm an assigned officer should consider:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures

- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology:
    - was used in relation to the information, and
    - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information
- the likelihood that the persons, or the kinds of persons, who:
    - have obtained, or who could obtain, the information, and
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates
    - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters

Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- 'sensitive information', such as information about an individual's health
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details)
- financial information
- a combination of types of personal information (rather than a single piece of personal information) that allows more to be known about the individuals the information is about

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the following:

- Whose personal information was involved in the breach?
- How many individuals were involved?
- Do the circumstances of the data breach affect the sensitivity of the personal information?
- How long has the information been accessible?
- Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?
- What parties have gained or may gain unauthorised access to the personal information?

In assessing the risk of serious harm, the assigned officer should consider the broad range of potential kinds of harms that may follow a data breach. It may be helpful to assess the likelihood of harm to consider a number of scenarios that would result in serious harm and the likelihood of each. Examples may include:

- identity theft
- significant financial loss by the individual
- threats to an individual's physical safety
- loss of business or employment opportunities

- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are also relevant considerations.

If Comcare acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, it would not be considered 'eligible' and therefore no requirement to notify any individuals or the Commissioner.

If an assigned officer believes that an incident meets the criteria above it should be raised with the AD or Director and if agreed proceed to notifying the individuals and OAIC.

Notifying individuals and OAIC of an eligible breach

Once we have reasonable grounds to believe there has been an eligible data breach, we must, as soon as practicable, make a decision about which individuals to notify, prepare a statement for the Commissioner and notify individuals of the contents of this statement.

9. The Assigned Officer should prepare a statement for OAIC. The OAIC's online form can assist in preparing this statement. This statement should be Quality assured by a Statutory Oversight AD prior to submission online.

The NDB scheme provides some flexibility for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity. If it is practicable:

- an entity can notify each of the individuals to whom the relevant information relates. That is, all individuals whose personal information was part of the eligible data breach or
- an entity can notify only those individuals who are at risk of serious harm from the eligible data breach.
- If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, then the entity must:
    - publish a copy of the statement on its website if it has one
    - take reasonable steps to publicise the contents of the statement

10. Although the assigned officer can use any method to notify individuals (for example, a telephone call, email, letter, or in-person conversation) the preference is a formal letter on Comcare letterhead. The notification must include the following information:
    - the identity and contact details of the entity
    - a description of the eligible data breach that the entity has reasonable grounds to believe has happened
    - the kind, or kinds, of information concerned
    - recommendations about the steps that individuals should take in response to the eligible data
11. Once the notification is drafted send to FOI@comcare.gov.au for QA by a Statutory Oversight AD.
12. Once the notification letter is approved, draft email to recipient ensuring:
    - the from field is Privacy@Comcare.gov.au ,
    - BCC yourself (to enable saving to file)
    - attach letter and place drafted email into the Drafts folder in the FOI mail box.

A Statutory Oversight AD will privacy check and send the email.

13. If options 1 or 2 are not practicable, the assigned officer should discuss with the Director of Statutiory Oversight. A decision will need to be made on whether it is appropriate, to publish a copy of the statement prepared for the Commissioner on Comcare's website and take reasonable steps to publicise the contents of that statement. A reasonable step when publicising an online notice, might include:
    - ensuring that the notice is prominently placed on the relevant webpage, which can be easily located by individuals and indexed by search engines
    - publishing an announcement on the entity's social media channels
    - taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach individuals at risk of serious harm

Recommendations and closing

14. If there are recommendations to ensure the practice or incident is not repeated enter them in the space provided on the form.

    Recommendations could include things like:

    - Removal or clean out of Auto-population function in Outlook
    - Creation/implementation of Quality Assurance steps for disclosures of information
    - Utilise Pracsys email function rather then emailing direct from outlook
    - Staff to attend privacy training

    Consideration of recommendations should not be limited to the individual(s) involved – the issue could be systemic and recommendations may need to be disseminated more broadly – assigned officer will need to think of all appropriate recommendations.

15. The completed incident report form should be sent to FOI@comcare.gov.au for QA.

16. Following QA, send the Privacy incident form to the relevant Director, team leader and reporting officer.

17. Once the incident has been finalised, the file can be closed. Please ensure:

    - All documents and correspondence is saved to the matter file in TRIM.

    - The incident is finalised in the Privacy Matter register.

Complaints

Overview

A complaint is an expression of dissatisfaction or concern about the Comcare's handling of Personal information and it is usually accompanied by a request to rectify the problem, whether explicit or implicit.

Complaints should be in writing, providing as much detail as possible, and addressed to privacy@comcare.gov.au.

The Statutory oversight team will take reasonable steps to investigate any complaint and provide response to the complainant within 30 days.

If we do not respond to the complaint within 30 days, or if the complainant is not satisfied with the outcome of their complaint, they can raise a complaint with the Office of the Australian Information Commissioner (OAIC).

Complaints Procedure

Call from complainants who will not identify themselves or wish to remain anonymous

Complainants who are unwilling or refuse to identify themselves are to be advised that we may not be able to respond to their complaint. This is due to needing to be informed about the information that has potentially been used, collected or disclosed and in ensuring we meet with our obligations under the Privacy Act.

Privacy Complaints relating to collection, use or disclosure by employers.

These complaints are not managed or investigated by Statutory Oversight. Complainants need to be advised that Statutory Oversight only manage privacy complaints involving Comcare's collection, use and disclosure of personal information, therefore the complainant needs to be directed the Privacy areas with their employers.

Privacy Complaints relating to Staff Claims

Privacy complaints relating to Staff Claims will only be managed by team members authorised to access to staff claims. If a staff member is concerned about submitting a complaint to the Privacy mailbox, they are encouraged to discuss the complaint or email directly to one of the statutory Oversight AD's or Statutory Oversight Director. It should be noted that the Privacy Mailbox is administered by the Director of Statutory Oversight.

Complaints relating to secure claims

Privacy complaints relating to Secure Claims will be managed by a Staturtory Oversight AD with authority to administer these claims. These types of complaints should be sent directly to the Director of Statutory Oversight team.

Notification and Acknowledgement

1. The Statutory Oversight Director will assign complaints to Statutory Oversight Officers.

2. Assigned officers are required to create a matter file in Trim.

    - Files are to be created under the Complaints Mega Folder (MF) within SC15/89
    - Register the matter in the corresponding Privacy Matter register (financial year) located in Trim file 2014/593.
    - All correspondence is to be saved to file.

    File creation process is outlined at Annexure IV.

3. Privacy complaints pertaining to claims within the Delegated Claims Management Arrangement (DCMA) are handled by the Statutory Oversight Team in line with the Comcare Delegated Claims Management Arrangements business processes (DCMA business processes) available on Comnet . The complaints procedure outlined in this document is to be followed

and the final response to the employee will also be sent to the Agency/Service Provider copying in the Delegated Claims Service team, DCSteam@comcare.gov.au

4. Is the Information involved about the person who is raising the complaint?

    - If yes, proceed to next step.

    - If no, clarify the complainant's authority to act (we will require authority (either orally or written) from the person whose information is involved in the complaint before responding or disclosing any information). If consent is not provided or cannot be obtained consideration of how to proceed with the complaint is to be discussed with an AD or the Director of Statutory Oversight.

5. The assigned officer, when practical, should call the complainant to confirm the concerns as well as to provide a timeframe for response. (30 Days)

6. An acknowledgement email should be drafted, outlining:

    - Your understanding of the complaint

    - The trim reference number

    - The estimated timeframe for response

    - Name and contact details of the assigned officer

7. The email, addressed from Privacy@comcare.gov.au is then placed into the draft folder of the foi@comcare.go.au mailbox for AD QA. The email should BCC the assigned officer so that it can be saved to the matter file.

Assessment:

The nature of complaints will vary, so an individual assessment of each complaint is essential in determining the best way to manage and prioritise matters.

8. The assigned officer needs to collect evidence of what has occurred. This can be from both the complainant and the business area involved. Statutory Oversight officers should only obtain further information where it is reasonably necessary to assess the complaint.

9. When undertaking an assessment of whether there has been an interference with privacy, Statutory Oversight officers should rely on source documents where they are available.

10. If input is required from other areas within Comcare this should be sought and filed within the relevant TRIM file. Provide three days for response.

    - Assessment needs to address the following:

    - What personal information is involved?

    - What has occurred (collection, use or disclosure)?

    - Why has it occurred?

- What APP is relevant to the concerns raised
- Has there been an interference with privacy?
- What, if any, steps to contain an interference occurred?
- All correspondence and file notes are to be saved to file.

Decision and Finalisation

All Privacy complaint decisions should be drafted using the template at Annexure V.

11. Assigned officer draft decision letter and include the following information:
    - Date of complaint
    - Complaint details
    - Relevant APP's
    - Summary of decision
    - Further complaint options
    - Name of decision officer
    - Statement of reasons
    - Information relied upon
    - Relevant Laws and guidelines
    - Findings
    - Conclusions
12. Save draft decision to file. file naming convention is:

    LAST NAME, Given name - Trim reference number - APP

13. Send Draft decision letter to FOI@comcare.gov.au for QA by Statutory Oversight AD.
14. At completion of QA, draft response email, attaching decision letter and ensure the From field is Privacy@comcare.gov.au
15. Place email into the draft folder of the foi@comcare.go.au mailbox for AD QA. The email should BCC the assigned officer so that it can be saved to the matter file.
16. Once the complaint decision has been notified, the file can be closed. Please ensure:
    - All documents and correspondence is saved to the matter file in TRIM.
    - The complaint is finalised in the Privacy Matter register

Privacy enquiries

A Privacy enquiry is a request for advice regarding any facet of privacy within Comcare. Privacy enquiries are made internally by telephone or email to privacy@comcare.gov.au.

Statutory Oversight will provide response to an enquiry within 10 days.

Privacy Enquiries Procedure

Privacy enquiries are received through privacy@comcare.gov.au. If an enquiry is received by phone, request that it be put in writing to the Privacy mailbox.

1. The Statutory Oversight Director will assign privacy incident matters to Statutory Oversight Officers.

2. Assigned officers are required to create a matter file in Trim.

    - Files are to be created under the Enquiry Mega Folder (MF) within SC15/89

    - Register the matter in the corresponding Privacy Matter register (financial year) located in Trim file 2014/593.

    - All correspondence is to be saved to file.

3. Assigned officer to draft response based on Privacy Act obligations, APP's and APP guidelines.

4. Draft response to be sent to FOI mailbox for AD QA.

5. Once QA complete, assigned officer email response to enquirer ensuring email is addressed from Privacy.

6. Once the enquiry response has been notified, the file can be closed. Please ensure:

    - All documents and correspondence is saved to the matter file in TRIM.

    - The complaint is finalised in the Privacy Matter register

Privacy enquiries also include requests for redaction of information from the Delegated Claims Management Arrangement Teams (Allianz and Gallagher Bassett). These requests follow the first two steps above (assignment, file creation and matter register) and then following apply:

1. The requesting officer should provide a folio number that requires the redactions, the assigned officer will need to locate the folio in Pracsys:

    - Open relevant claim file in Pracsys

    - Select the Electronic tab to display all documents within the file

    - Locate folio - note document number (This will be required to save the Document back in to the claim file).

2. To enable redactions, the folio will need to be saved outside of Pracsys

- Tag folio and select print folio
- Save to desktop or document folder

3. Open document in Adobe Acrobat Pro from the Tools tab, under Protect & Standardize, select Redact
4. Select properties and set appearance to the following:
    - Redacted area fill colour – white
    - Use Overlay Text
    - Overlay text – Helvetica, font size 10
    - Alignment Left
    - Custom Txt – APP4
    - Redaction Mark Appearance - Outline colour Red
5. Select Mark for Redaction – Text and Images – Click OK
6. Locate and select information requiring redaction (information selected will have red outline applied)
7. Once all information has been marked for redaction, select apply. Click Ok when prompted an select no when asked 'would you like to also find and remove hidden information in your document?'
8. Save document to Desktop/Document folder
9. Conduct a record number search within TRIM and enter the relevant DOC number.
10. Drag the redacted document over the top of the document in trim. You will then be prompted to save it as a new revision – Select OK.
11. Draft response email to the requesting officer, ensure the From field is Privacy@comcare.gov.au
12. Place email into the draft folder of the foi@comcare.go.au mailbox for AD QA. The email should BCC the assigned officer so that it can be saved to the matter file.
13. Once the complaint decision has been notified, the file can be closed. Please ensure:
    - All documents and correspondence is saved to the matter file in TRIM.
    - The complaint is finalised in the Privacy Matter register

Privacy Impact Assessments

Overview

A privacy impact assessment (PIA) is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. The term Project is intended to cover the full range of activities and initiatives that may have privacy implications including:

- policy proposals
- new or amended programs, activities, systems or databases
- new methods or procedures for service delivery or information handling
- changes to how information is stored.

Undertaking a PIA can assist Comcare to:

- describe how personal information flows in a project
- analyse the possible impacts on individuals' privacy
- identify and recommend options for avoiding, minimising or mitigating negative privacy impacts
- build privacy considerations into the design of a project
- achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.

A large part of a project's success will depend on whether it meets legislative privacy requirements and community privacy expectations. Privacy issues that are not properly addressed can impact on the community's trust in Comcare and undermine the project's success.

Procedures – Threshold Assessment

The first step in undertaking a PIA is assessing whether a PIA is necessary for the project. Not every project will need a PIA.

Comcare's project management design incorporates a review process for privacy. The Statutory Oversight team is notified when new project business cases are raised in Comcare's project management database Jumpstart. When projects involving the handling of personal information are identified, the project manager will be required, as a first step to undertake a threshold assessment.

A threshold assessment is used to determine whether it will be necessary to undertake the rest of the steps involved in a PIA.

1. The Assigned Officer (AO) is required to create a matter file in Trim

    - Files are to be created under the Privacy Impact Assessment Mega Folder (MF) within SC15/89

    - register the matter in the corresponding worksheet of the Privacy Matter register (financial year) located in Trim file 2014/593.

- All correspondence is to be saved to file.

File creation process is outlined at Annexure IV

2. The threshold assessment template is provided to the project manager by the Statutory Oversight team. The Project Manager must complete the following sections:

    - Brief description of the project and project objective
    - Consideration of whether the project involves the collection, storage, use or disclosure of personal information:
        - brief description of the personal information (if any) that will be collected, used or disclosed (such as name, address, date of birth, health information and so on)
        - source of personal information (e.g. whether the personal information is sourced from existing claim data, or whether the personal information is collected from new sources).
        - disclosure of information to any third parties
    - Involvement of personal information:
        - how any personal information will be used.
    - key privacy elements:
        - the nature and sensitivity of the personal information.
        - any authority under which personal information is collected
        - any changes to the way personal information will be handled

Once the Threshold assessment has been completed by the project manager, an Assigned Officer in the Statutory Oversight Team will review and complete the following sections:

- Management of privacy risks
    - What are the risks
    - how they will be managed
- Consideration of compliance with the APP's
    - does the project comply with the APP's

CONCLUSION

The Assigned Officer, considering all of the information will determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts.

A negative privacy impact may not appear to be significant, but it is important to note that even minimal personal information, handled inappropriately, may impact on someone's privacy in ways Comcare did not intend. The conclusion will include:

- Assessment of whether a full Privacy Impact Assessment is required

- Recommendations about how to manage/mitigate risk
- Details of the person or team responsible for completing the threshold assessment and the Officer endorsing

The draft report will be sent to FOI@comcare.gov.au to be cleared by another AD or the Director of Statutory Oversight.

Once cleared, the draft threshold assessment report will be provided to the Project Manager for their review and input. Any questions or comments raised by the Project Manager should be addressed by the AD.

Once all issues have been addressed, a final report must be sent to the Project Manager from the Privacy@comcare.gov.au.

Once the Threshold assessment is finalised and there is no recommendation for a full PIA, the file can be closed. Please ensure:

- All documents and correspondence is saved to the matter file in TRIM.
- The PIA Threshold assessment is closed in the Privacy Matter register

Procedures - Undertaking a Full Privacy Impact Assessment

When it has been concluded in the threshold assessment that a full PIA is necessary, the following will be considered, and all documentation is to be saved to the file created for the threshold assessment:

There are nine distinct steps within the PIA process.

1. Planning

Planning the full PIA should consider a range of elements, including:

- how detailed the PIA needs to be, based on a broad assessment of the project and its privacy scope
- who will conduct the PIA
- the timeframe for the PIA
- the budget and other resources available for the PIA
- the extent and timing of stakeholder and public consultations
- steps that will need to be taken after the PIA, including implementation of recommendations and ongoing monitoring.

The project's nature and stage of development will have an impact on how detailed the PIA process needs to be. A project may be at a conceptual or a more advanced stage of development, be an 'incremental' program (altering a well-established existing program) or a significant new one, and have a limited or broad scope.

The size or budget for a project is not a useful indicator of its likely privacy impact, and even a small-scale project may have significant privacy implications. When assessing the project's privacy scope, you will need to look at its key attributes, including:

- the quantity of personal information handled

- whether sensitive information is involved
- the size or complexity of the project
- whether the project will involve cross-organisation/agency or cross-sector information sharing
- the likely community and/or media interest in the privacy aspects of the project.
- A project's privacy scope can increase depending on the risk of privacy impacts, for example, in circumstances where:
- personal information handling will be or has been outsourced
- new legislation or new technology will be needed for handling or storing the personal information
- personal information will be aggregated in databases
- the personal information will be used for data-matching
- entirely new collections of personal information are planned
- a new method of using or disclosing personal information is planned
- provision of personal information will be compulsory
- the handling of personal information will have an impact on key aspects of an individual's life (such as livelihood, housing, reputation, health), or individuals may experience adverse outcomes (such as fines, reduction or cancellation of entitlements) as a result of the collection or use of their personal information.

Generally, the greater the privacy scope of the project, the more likely it will be that the PIA will need to be more detailed, to better determine and manage the project's privacy impacts.

Identifying who will conduct the PIA

Generally, whoever is managing the project would be responsible for ensuring the PIA is carried out. The nature and size of the project will influence the size of the team needed to conduct the PIA, and how much the team needs to draw on external specialist knowledge.

The Statutory Oversight Team will lead all full PIA and will make use of 'experts' including information security, technology, risk management, operational procedures and industry-specific knowledge.

Where a project will have a substantial privacy impact an independent PIA conducted by an external assessor may be required. If this is required a procurement exercise will be conducted by Statutory Oversight and the Project Manager.

2. Describe the project

A PIA needs a broad, 'big picture' description of the project, including:

- the project's overall aims
- how these aims fit with the organisation or agency's broader objectives
- the project's scope and extent
- any links with existing programs or other projects

- who is responsible for the project
- timeframe for decision-making that will affect the project's design
- some of the key privacy elements – for example, the extent and type of information that will be collected, how security and information quality are to be addressed, and how the information will be used and disclosed (these will be explored in more detail in subsequent stages of the PIA).

The project description should be sufficiently detailed to allow external stakeholders to understand the project, and should be written in plain English, avoiding overly technical language or jargon.

3. Identify and consult with stakeholders

Stakeholders are those who are or might be interested in or affected by the project being considered. It is likely that Comcare will have internal stakeholders and external stakeholders, including regulatory authorities, clients, advocacy organisations, service providers, industry experts, academics and others. The stakeholder list should identify both categories of stakeholders, and individuals and organisations within each of these categories. It may be necessary to add to the stakeholder list as the project progresses.

Identifying the project's stakeholders will assist when undertaking consultation on the PIA. It may not be necessary to consult with all the identified stakeholders, depending on the scale and likely privacy impacts of the project, but some form of consultation should occur as part of the PIA.

Consulting with stakeholders may also assist in identifying privacy risks and concerns that have not been identified by the team undertaking the PIA, and possible strategies to mitigate these risks.

Consultation may also offer stakeholders the opportunity to discuss risks and concerns with the entity and to gain a better understanding of, and provide comment on, any proposed mitigation strategies. Importantly, consultation is also likely to provide confidence to the public that their privacy has been considered.

4. Map information flows

After a broad outline of the project's nature and scope has been prepared, a description and map the project's personal information flows is required. The analysis should be sufficiently detailed to provide a sense of what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it.

To map information flows effectively the assigned officer will need to consult with subject matter experts and project stakeholders.

Detailed information mapping should include:

- whether identity verification will be necessary
- what personal information will be collected and how it will be collected
- its use and disclosure
- the processes for ensuring information quality

- security safeguards that are (or will be) in place
- the ability individuals have to access and correct their personal information.

Mapping should also describe the current personal information environment and how the project will affect it.

Areas for consideration when you are mapping the information flows are outlined below. These points will help describe how the project deals with each of these areas and draw attention to any privacy issues. The responses should be documented and used in the privacy impact analysis stage. They will also be useful for the preparation of the PIA report.

If appropriate, consider using diagrams depicting the flow of information, or tables setting out the key information for different types of personal information to be used in the project.

Necessity of identity verification

Identify and describe:

- the extent to which the project can proceed using anonymous or de-identified information
- whether it is necessary to verify identity, and the degree of confidence needed
- how identity will be verified
- other information that may need to be verified, such as an individual's qualifications.

Collection

Identify and describe:

- the personal information to be collected, including any sensitive information
- how the collection relates to the agency or organisation's functions or activities
- why the personal information, including the particular items and kinds of information, is necessary for the project
- whether the information can be collected in a de-identified or anonymous way
- whether individuals can choose not to provide some or all of the personal information

Detail the collection process, including (but not limited to):

- how the information will be collected (for example, hard copy forms, electronic forms, online transactions, CCTV etc)
- whether unsolicited personal information may be used in the project
- where the information will be collected from (for example, directly from the individual, from other individuals or entities, or from publicly available sources)
- any legislation or other authority on which you are relying to collect the information
- collection alternatives that have been considered and rejected (for example, using de-identified information)

- how often the personal information is to be collected (once only or ongoing)
- any limits on the nature of the information to be collected (for example, information over a certain age)

Identify and describe information (notice) about collection to be given to the individual and how it will be given, including:

- Purpose and authority
    - why the personal information is being collected
    - whether the collection is authorised or required by law, and if so, which law.
- Use and disclosure
    - uses or disclosures that you consider consistent with the purpose for collection
    - the people or organisations to which you usually or sometimes disclose personal information, and any further uses or disclosures that are made by those people or organisations
    - proposed uses or disclosures of the information for purposes other than the purpose of collection.
- Choice
    - whether there are choices for individuals about how their personal information is handled, and if so, whether you will inform them.

Use

Identify and describe how you intend to use the information:

- all the planned uses of the personal information, including infrequent uses
- how all these uses relate to the purpose of collection
- measures in place to prevent uses for secondary purposes or to ensure that any secondary uses are permitted under the APPs.

If information may be used for a secondary purpose, identify and describe:

- whether consent is required for the secondary use
- if the use is related or directly related to the purpose of collection
- whether an individual can refuse consent for secondary uses and still be involved in the project
- any consequences for individuals who refuse consent
- how individuals will be involved in decisions if new, unplanned purposes for handling personal information occur during the project.

Data linkage or matching, which involves aggregating or bringing together personal information that has been collected for different purposes, has additional privacy risks. If your project will involve data linkage or matching, identify and describe:

- any intention or potential for personal information to be data-matched, linked or cross-referenced to other information held in different databases (by you or other entities)
- how data-matching, linking or cross-referencing might be done
- any decisions affecting the individual that might be made on the basis of data-matching, linking or cross-referencing
- safeguards that will be in place to limit inappropriate access, use and disclosure of the information
- audit trails and other oversight mechanisms that will be in place
- protections in place to ensure data linkage accuracy and that individuals will not be adversely affected by incorrect data matching.

Disclosure

Identify and describe:

- to whom, how and why the personal information will be disclosed
- whether the disclosed information will have the same privacy protections after it is disclosed
- whether the information is to be published, or disclosed to a register, including a public register
- whether an individual will be told about the disclosure and what choices they have (such as publishing or suppressing their information)
- whether the disclosure is authorised or required by law, and if so, which law
- whether the personal information will be disclosed to overseas recipients.

Information quality

Identify and describe:

- the consequences for individuals if the personal information is not accurate or up-to-date, including the kinds of decisions made using the information and the risks of using inaccurate information
- the processes that ensure only relevant, up-to-date and complete information will be used or disclosed, including by any contracted service providers
- how personal information updates will be given to others who have previously been given personal information about an individual.

Security

Assess the project against your agency or organisation's IT, telecommunications and physical security measures

Identify and describe:

- security measures that will protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse (including for contracted service providers)
- how information will be transferred between sites
- how personal information will be protected if it will be managed by someone else
- who will have access
- who will authorise access
- the systems that will prevent and detect misuse or inappropriate access
- what action will be taken if there is a data breach.

Retention and destruction

Identify and describe:

- when personal information will be de-identified or destroyed
- how this will be done securely
- whether an information retention policy and destruction schedule is in place
- how compliance with this policy and any relevant legislation about record destruction will be assessed.

Access and correction

Identify and describe:

- how individuals can access their personal information, including any costs to the individual
- how the individual can have their personal information corrected, or annotations made, if necessary
- how decisions will be made about requests from individuals for access to or correction of their information.

5. Privacy impact analysis and compliance check

Once information flows have been mapped, the next step is to identify and critically analyse how the project impacts upon privacy, both positively and negatively.

Privacy impact analysis investigates:

- the risk of privacy impacts on individuals (both serious and more minor) as a result of how personal information is handled
- whether privacy impacts are necessary or avoidable
- whether there are any existing factors that have the capacity to mitigate any negative privacy impacts
- how the privacy impacts may affect the project's broad goals

- the project's effect on an individual's choices about who has access to their personal information
- compliance with privacy law
- how the use of personal information in the project aligns with community expectations.

Ultimately, the privacy impact analysis should attempt to determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts.

The analysis should include consideration of the content of the information and the context in which the information is collected. A negative privacy impact may not appear to be significant, but it is important to note that even minimal personal information, handled inappropriately, may impact on someone's privacy in ways an entity did not intend.

Some key questions to consider are:

- Do individuals have to give up control of their personal information?
- Will the project change the way individuals interact with the entity, such as through more frequent identity checks, costs, or impacts on individuals or groups who do not have identity documents?
- Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)?
- Is there a complaint-handling mechanism? If yes, is it visible, comprehensive and effective?
- How will you handle any privacy breaches?
- Are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?
- Does the project recognise the risk of function creep? (For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?)
- How valuable would the information be to unauthorised users? (For example, is it information that others would pay money for or try to access via hacking?)

Ensuring compliance

It is essential to consider compliance against the Privacy legislation, but consideration should also be given to other rules that may apply, such as information handling obligations in other legislation.

For each APP, consider whether your project complies and identify any risks to compliance. It should be documented, and specific details provided about either how the project complies with the APP or why you are not required to comply with an APP, and any considerations taken into account.

The Assigned Officer will need to consider whether the project complies with each of the APPs. For each APP, consideration needs to be given on whether the project complies and identify any risks to compliance. The Assigned Officer will need to provide specific details about either how the project complies with the APP or why Comcare is not required to comply with an APP, and any considerations you took into account.

APP 1—open and transparent management of personal information

Comcare must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.

- Have reasonable steps been taken to implement practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code?
- Does Comcare have an APP Privacy Policy which: is clearly expressed and up-to-date, is freely available at no cost?
- Have reasonable steps been taken to ensure that procedures and systems are in place for handling privacy inquiries and complaints?

APP 2—anonymity and pseudonymity

Individuals must have the option of not identifying themselves or if using a pseudonym, when dealing with Comcare in relation to a particular matter unless an exception applies.

- Will individuals have the option of not identifying themselves or of using a pseudonym when participating in the project?
- Are you required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves?
- Is it impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym?
- Are there categories of individuals affected by the project who are likely to seek to interact with your agency or organisation anonymously or using a pseudonym?

APP 3—collection of solicited personal information

Any personal information collected (other than sensitive information) must be reasonably necessary for or directly related to one or more of Comcare's functions or activities.

Comcare must not collect sensitive information about an individual unless an exception applies, such as if the individual consents and the information is reasonably necessary for or directly related to one of more of Comcare's functions or activities.

Personal information:

- is the information being collected necessary for or directly related to one or more of your functions?
- Is the collection authorised or required by an Australian law or a court/tribunal order?
- Will the information be collected by lawful and fair means?
- Will the personal information be collected from the individual concerned?

Sensitive information:

- Can you rely on any of the exceptions in APP 3.3 or APP 3.4 for the collection of sensitive information? For example, has the individual consented or is the collection required or authorised by or under an Australian law or a court/tribunal order?

- Will there be guidance or processes in place to assist with the handling of sensitive information?

- If the collection and management of sensitive information will be outsourced, will measures be in place to protect the sensitive information and will compliance be monitored?

APP 4—dealing with unsolicited personal information

Where Comcare receives unsolicited personal information, it must determine whether it would have been permitted to collect the information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, Comcare must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

- Are there practices, procedures and systems in place for dealing with the receipt of unsolicited personal information that will ensure compliance with APP 4?

APP 5—notification of the collection of personal information

If Comcare collects personal information about an individual, we must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2. The matters include:

- Comcare's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences if personal information is not collected
- Comcare's usual disclosures of personal information of the kind collected by Comcare information about Comcare's APP Privacy Policy
- whether Comcare is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

Comcare must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

Questions to consider:

- Consider each of the matters listed in APP 5.2.Will steps be taken to notify the individual of each matter? If steps are not being taken in relation to a matter, is it reasonable in the circumstances not to notify the individual?
- Are practices, procedures and systems in place to ensure reasonable steps are taken to tell the individual about the matters listed in APP 5.2 at or before (or if not practicable, as soon as practicable after) the time of collection?
- If the information is collected directly from the individual, will notice be given to the individual (such as by displaying the notice on a form, providing a link on a web page or advising the individual over the phone) and the individual asked to confirm they have been notified of the APP 5 matters before providing their personal information?

APP 6—use or disclosure of personal information

Comcare can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.

- If the use or disclosure is for a secondary purpose, will the individual be asked to provide consent? Will you keep a record of the consent?
- If the individual will not be asked to consent, do any of the other exceptions to the requirement for consent in APP 6.2 apply?
- Is it possible that personal information may be used or disclosed because it is reasonably necessary for an enforcement related activity? If so, are procedures in place to ensure a written note of the use or disclosure?

APP 7—direct marketing—irrelevant to comcare (not applicable)

An organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented. An organisation must provide its source for an individual's personal information, if requested to do so by the individual.

APP 8—cross-border disclosure of personal information

Before Comcare discloses personal information to an overseas recipient, we must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.

- If Comcare that discloses personal information to an overseas recipient we are accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs
- If personal information is to be disclosed to an overseas recipient, will reasonable steps be taken to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?
- Does an exception apply? For example, is the disclosure required or authorised by or under an Australian law or a court/ tribunal order?
- If no exception applies, are appropriate arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs?

APP 9—adoption, use or disclosure of government related identifiers

An organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies.

APP 10—quality of personal information

Comcare must take reasonable steps to ensure that the personal information we collect is accurate, up-to-date and complete. Comcare must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

- Will reasonable steps be taken to ensure that any personal information collected is accurate, up-to-date and complete? Will guidance or processes be in place to ensure these steps are followed?

- Will reasonable steps be taken to ensure that any personal information being used or disclosed is accurate, current, complete and relevant, having regard to the purpose of the use or disclosure? Will guidance or processes be in place to ensure these steps are followed?

APP 11—security of personal information

Comcare must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

- Will reasonable steps be taken to ensure that the personal information to be collected is protected from unauthorised access, modification or disclosure? Consider whether reasonable steps will be taken to ensure technical and physical security is in place to protect against misuse, interference and loss, and whether there will be technical and physical security guidance/processes in place.
- Will control procedures be in place requiring authorisation before personal information is added, changed or deleted?
- Will audit mechanisms identify inappropriate system access?
- Will reasonable steps be taken to destroy or de-identify the personal information which is no longer needed for any authorised purpose?
- If reasonable steps will not be taken to destroy or de-identify the personal information which is no longer needed for any authorised purpose, do any of the exceptions apply (for example, the information is part of a Commonwealth record or is Comcare required by law or a court/tribunal order to retain the information)?
- Will guidance or processes be in place to help determine when and how destruction or de-identification of personal information will occur?
- Is staff training adequate to fulfil the reasonable steps required?

APP 12—access to personal information

If Comcare holds personal information about an individual, Comcare must give the individual access to that information on request, unless an exception applies.

- Will processes be put in place to: generally provide an individual with access to information being held about them
- deal with requests for access within 30 days
- give access in the manner requested, if reasonable and practicable
- ensure the individual is advised of other means of access where a request is refused
- ensure a written notice is given to an individual whose access request is refused?
- Will individuals be made aware of how to access their personal information?

APP 13—correction of personal information

- Comcare must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.
- Will individuals be made aware of how to request correction of their personal information?
- Will reasonable steps be taken to correct information that is not accurate, out of date, incomplete, irrelevant or misleading, having regard to the purpose for which the information is held?
- Are processes in place for responding to requests from individuals to correct personal information?
- Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?
- Will individuals be informed about the reasons if a request for correction is denied?
- Are processes in place for associating a statement with personal information if a request for correction is denied?

6. Privacy management — addressing risks

The privacy impact analysis and compliance check may have identified risks to privacy in the project's current design. Risks to privacy can arise in many circumstances, for example, from collecting more information than is needed, using intrusive means of collection, or disclosing sensitive details more widely than is justified or necessary. These risks may be to individual privacy, to an entity's compliance and reputation, or both.

At this stage, considerations will now focus on options that may allow you to remove, minimise or mitigate any negative privacy impacts identified through the privacy impact analysis.

This does not necessarily mean compromising the goals of the project. There may be options that will make a significant difference to the privacy impact and still allow you to achieve the project's goals.

A number of factors should be taken into account when considering strategies for dealing with negative privacy impacts identified in the privacy impact analysis stage, including:

- necessity — minimising the collection of personal information to what is strictly necessary
- proportionality — any negative privacy impact should be in proportion to, or balanced with, any benefits to be achieved from the project
- transparency and accountability — privacy measures should be transparent to individuals, through adequate collection notices and privacy policies
- implementation of privacy protections — consider how organisational/agency policies and procedures can support privacy, as well as practical elements such as staff training
- flexibility — take into account the diversity of individuals affected by the project, and whether they may respond or be affected differently to the sharing of their personal information

- privacy by design — privacy protections should be included in law or other binding obligations, and built into new technologies
- privacy enhancing technologies — consider whether any privacy enhancing technologies can be used in the project, and the impact of privacy invasive technologies.

Strategies to reduce or mitigate privacy risks may include technical controls (for example, access control mechanisms, encryption, design changes), more operational controls (for example, organisational/agency policies or procedures, staff training, oversight and accountability measures) or communication strategies (for example, privacy notices).

Below is possible mitigation strategies for common privacy risks.

Possible risks	Possible Mitigation Strategies
Anonymity and pseudonymity: Individual's personal information will be collected when it is not required (for example, to provide information)	Consider whether you can use information that does not identify a person. If it is necessary to distinguish between different people, consider whether you can use pseudonyms instead.
Collection: Personal information will be collected without a clear purpose, which could increase the risk of unauthorised uses and disclosures.	Ensure that you have clearly identified and documented the purposes for which you will be collecting and using personal information, and that others in your organisation or agency are aware of these purposes.
Collection: Unjustifiably intrusive methods will be used to collect personal information	Consider other, less intrusive options for collecting the information. If these options are not suitable, the reasons should be documented in the PIA report.
Notification of collection: Collection notice will not be provided to all individuals, for example those using non-standard communication channels	Ensure that the collection notice is consistent and accessible across all methods of collection, including hard-copy forms, online forms and via telephone. Provide a post-collection notice where notice prior to or at the time of collection is not practicable.
Notification of collection: Collection notice may not be accessible to all consumers, for example those from culturally and linguistically diverse backgrounds	Ensure that the collection notice is available in a range of formats and an appropriate range of languages for the target group.
Collection, use or disclosure: Consent for collection, use or disclosure of information may not be valid	Review the process by which you plan to seek consent. Ensure that the consent will be truly voluntary, informed, current and specific, and given by a person with the capacity to provide consent.
Use or disclosure: Individuals may be surprised or upset by a secondary	Undertake further stakeholder consultation to test community expectations about your proposed uses and

Possible risks	Possible Mitigation Strategies
use or disclosure, resulting in privacy complaints and/or negative publicity	disclosures. Consider whether it is possible to seek consent for secondary uses and disclosures.
Disclosure: De-identification of personal information before disclosure may not prevent re-identification	Review de-identification procedures to ensure that sufficient details are removed so that the recipient of the information will not be able to re-identify it, or combine it with other information to establish an individual's identity.
Information quality: Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	Check the reliability of tools used to collect or process personal information. Consider establishing regular checks of tools and procedures for human data processing. Identify and document procedures for how often personal information will be reviewed and updated.
Information security: The organisation or agency does not have basic information security standards in place.	Review the OAIC's *Guide to information security* and identify what additional steps your organisation or agency needs to take to ensure protection of personal information.
Information security: Information is saved onto personal storage devices, increasing the risk of accidental loss of personal information.	Control the use of portable storage devices through organisational/agency policies and technical controls.
Access and correction: Individuals are not able to easily access and correct their personal information.	Identify how access and correction procedures can be made more straightforward. Consider providing individuals with routine access to their personal information.

7. Recommendations

A number of recommendations for the future of the project may emerge from the stages above. These recommendations should identify avoidable impacts or risks and how they can be removed or reduced to a more acceptable level. For example, recommendations could address:

- changes that would achieve a more appropriate balance between the project's goals, the interests of affected individuals and the entity's interests
- privacy management strategies, discussed above in 'Privacy management — addressing risks', that will reduce or mitigate privacy risks
- the need for further consultation
- whether the privacy impacts are so significant that the project should not proceed.

Recommendations might also go beyond project-specific matters to overall privacy risk management for the entity conducting the project.

Recommendations should be set out in the PIA report. It should be clear who the recommendations are addressed to, for example to different areas of the organisation or agency, particular members

of the project team, or those in positions of authority within the organisation or agency. Recommendations should also include a timeframe for implementation.

8. Report

A report that sets out all the PIA information should be completed. Key elements for inclusion in a PIA report include:

- Executive Summary
  - the purpose of the PIA
  - brief project description and key information flows
  - summary of findings
  - recommendations or existing strategies to address identified privacy risks.
- project description
  - describe the key features of the project, including any relevant background or the rationale for the project. Outline how personal information will be handled in the project, including through diagrams illustrating information flows if appropriate.
- PIA methodology
  - outline the approach taken to undertaking the PIA, including any stakeholder consultation.
- description of information flows
- outcome of privacy impact analysis and compliance checks, including positive privacy impacts and privacy risks that have been identified, and strategies already in place to protect privacy
- recommendations to avoid or mitigate privacy risks
- description of any privacy risks that cannot be mitigated, the likely community response to these risks, and whether these risks are outweighed by the public benefit that will be delivered by the project
- if necessary, more detailed information (for example about consultation processes and outcomes) can be provided in appendices.

The drafted report should be sent to FOI@comcare.gov.au to be cleared by another AD or the Director of Statutory Oversight.

Once cleared, the PIA report will be provided to the Project Manager for their review and response to recommendations raised in the report.

Any questions or comments regarding the report or recommendations will need to be raised with Statutory Oversight and should be addressed by the assigned officer.

9. Respond and review

It is important that action is taken to respond to the recommendations raised in the report, and to continue to review and update the PIA. A PIA should be regarded as an ongoing process that does not end with the preparation of the PIA report.

Responding to recommendations in a PIA is one of the most important aspects of the process and will lead to better privacy outcomes. The project manager may make a decision not to implement all the recommendations set out in the PIA report. However, they should document which recommendations they intend to implement (or have already implemented), as well as those which they do not intend to implement and the rationale for this decision.

Ideally, the response to the PIA recommendations will be published together with the PIA report. If a PIA report is not published, consideration should be given to providing it to significant stakeholders to assist in effective implementation of recommendations.

It may be helpful to prepare a plan for implementing the recommendations, indicating a specific timeframe for remedying or mitigating the risks that have been identified and identifying who is responsible for the implementation. An implementation document should be attached to the PIA report or saved to the PIA file.

Consideration should also be given to ongoing management of any privacy risks inherent in the project. This could be incorporated into an entity's overall risk management strategy.

Once all issues have been addressed, a final report must be sent to the Project Manager from the Privacy@comcare.gov.au.

Once the PIA is finalised, the file can be closed. Please ensure:

- All documents and correspondence (including recommendations and implementation documentation) is saved to the matter file in TRIM.
- The PIA is closed in the Privacy Matter register

APP12 Access to personal information

Overview

Under APP12, an individual can request access to their personal information. Comcare must, if we hold information about an individual and on request, give that individual access to the personal information (APP 12.1). There are however grounds on which access may be refused, for Comcare (as an agency) if we have reasons to refuse access under the FOI Act we are able to use those for a APP12 request.(see refusal of APP12 requests below)

APP12 does not stipulate formal requirements for making a request, or require that a request is made in writing or require the individual state that it is an APP12 request.

APP 12 also sets out minimum access requirements, including a 30 day time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

Comcare must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record.

Factors relevant in assessing whether it is reasonable and practicable to give access in the manner requested by an individual include:

- the volume of information requested. For example, it may be impracticable to provide a large amount of personal information by telephone.

- the nature of the information requested. For example, it may be impracticable to give access to digitised information in hard copy and it may be unreasonable to give access to information of a highly sensitive nature by telephone if the APP entity cannot sufficiently verify the individual's identity over the telephone.

- any special needs of the individual requesting the information. For example, it may be reasonable to give information in a form that can be accessed via assistive technology where this meets the special needs of the individual.

There is no right to a review an APP12 decision. Applicants can make a complaint that there has been an interference with their privacy under the Privacy Act to the Information Commissioner.

APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an APP entity from giving access to personal information under an informal administrative arrangement, provided the minimum access requirements stipulated in APP 12 have been met.

APP 12 Procedure

1. The Statutory Oversight Director will assign APP 12 requests to Statutory Oversight Officers.
2. Assigned officers are required to create a matter file in Trim.
    - Files are to be created under the APP12 and 13 Requests Mega Folder (MF) within SC15/89
    - Register the matter in the corresponding worksheet in the Privacy Matter register (financial year) located in Trim file 2014/593.
    - All correspondence is to be saved to file.

    File creation process is outlined at Annexure IV
3. Draft acknowledgement email to the applicant. Email should include:
    - Outline of information requested
    - The trim reference number assigned to the request
    - The timeframe for response
    - Name and contact details of the assigned officer
4. The email, addressed from Privacy@comcare.gov.au is then placed into the draft folder of the foi@comcare.go.au mailbox for AD QA. The email should BCC the assigned officer so that it can be saved to the matter file.

5. Email all business areas that may hold the requested personal information. Undertaking preliminary searches, including of CM9, will assist the allocated officer to identify relevant business areas. The email, addressed from privacy@comcare.gov.au should include:
    - What information has been requested
    - Timeframe for response – Three days

    Save email to Trim file.

6. Once responses are received the allocated officer will need to review all personal information ensuring it meets the scope of the request.
7. Information meeting scope will need to be combined and saved to the Trim File.
8. Allocated Officer should consider if a refusal reason exist (see next step). Where the request is straight forward and documentation clearly does not meet refusal continue to step 10:

Authority to refuse access under the FOI Act

The FOI Act lists several grounds on which an agency can refuse a request under the Act for access to documents. An agency may rely on any of those grounds to refuse access under APP 12. It is nevertheless open to an assigned Officer to not to rely on any such ground and to provide access upon request, unless disclosure is prohibited.

The grounds on which an access request can be declined under the FOI Act include:

- a document is an exempt document under Part IV, Division 2 of the FOI Act, for example, the document is a Cabinet document, is subject to legal professional privilege, contains material obtained in confidence, or a secrecy provision applies

- a document is a conditionally exempt document under Part IV, Division 3 of the FOI Act, for example, the document contains deliberative matter, or disclosure of the document would involve the unreasonable disclosure of personal information about another person and it would be contrary to the public interest to release the document at that time

- the individual is not entitled to obtain access to a document of the kind requested, for example, the document is available for purchase from an agency (FOI Act, ss 12, 13)

- providing access in the terms requested by a person would substantially and unreasonably divert an agency's resources from its other operations (s 24AA)

- processing a person's request would require an agency to disclose the existence or non-existence of a document, where that would otherwise be exempt information (s 25)

The FOI Act specifies consultation processes that may apply to requests made under that Act, for example, where a 'practical refusal reason' may apply (FOI Act, s 24) to the request, or where a requested document contains a third party's personal or business information (FOI Act, ss 27, 27A).

An agency is not required to undertake any of those consultation processes before refusing access on any of those grounds under APP 12. This is required only if the person decides to make a request under the FOI Act.

9. Where a practical refusal reason exists for voluminous requests, the allocated officer will be required to conduct a 10% sample of documents. The following steps will need to be taken:

    - Calculate the size of the request (files, pages, documents)
    - Review 10% of documents for possible exemptions required.
    - Enter data into the FOI Charges calculator (Annexure VI) to predict hours required to fulfil request

    Save all sampling evidence to file.

10. Draft APP 12 decision letter. Decision letter must include:

- The decision to grant access or refuse access
- Set out the reasons for the any refusal
- Complaint mechanisms available to the individual

An example decision notice is at Annexure VII

11. Save draft decision to file. file naming convention is:

    - LAST NAME, Given name - Trim reference number – APP12 Notice

12. Send Draft decision letter to FOI@comcare.gov.au for QA by Statutory Oversight AD.
13. At completion of QA, save finalised notice as PDF.
14. Draft response email, attaching decision letter and ensure the From field is Privacy@comcare.gov.au. The email should BCC the assigned officer so that it can be saved to the matter file.
15. Place email into the draft folder of the foi@comcare.go.au mailbox for AD QA.
16. Once the decision has been notified, the file can be closed. Please ensure:

    - All documents and correspondence is saved to the matter file in TRIM.
    - The APP12 request is finalised in the Privacy Matter register

APP13 Requests

Overview

APP 13 sets out minimum procedural requirements for the correction or annotation of personal information, these are not as detailed as the FOI Act provisions.

APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

- This requirement applies where:
    - the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
    - the individual requests the entity to correct the personal information
- Special considerations apply to Commonwealth records, which can only be destroyed or altered in accordance with the Archives Act 1983 (Archives Act).
- APP 13 also sets out other minimum procedural requirements in relation to correcting personal information, including when an APP entity must:
    - take reasonable steps to notify other APP entities of a correction

- give notice to the individual which includes reasons and available complaint mechanisms if correction is refused
- take reasonable steps to associate a statement with personal information it refuses to correct
- respond to a request for correction or to associate a statement, and
- not charge an individual for making a request, correcting personal information or associating a statement

- APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including informal arrangements and, for agencies, the Freedom of Information Act 1982 (FOI Act).

Where we are satisfied that the information is incomplete, incorrect, out-of-date, misleading or irrelevant, we may amend the record. We are not obliged to amend the record. But where we do agree to amend a record, we must, as far as possible, retain the text of the record as it was prior to the amendment.

Where an amendment request is refused, we must provide reasons for the refusal. We must also give an individual the opportunity to make a statement expressing their disagreement with the record and we are obliged to annotate the record, by attaching that statement—unless we consider the statement to be irrelevant, defamatory or unnecessarily voluminous.

There are no formal requirements for making a request under APP13 and we cannot charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement.

Comcare must respond to a request to correct a record or to associate a statement within 30 calendar days. The 30-day time period commences on the day after the day the agency receives the request.

Generally there are two ways an APP13 Correction request will be raised with the Statutory Oversight Team:

- An individual makes a request
- A Comcare Officer may become aware that an item of personal information requires correction when they discover an inconsistency during normal business practices. Examples include:
  - information provided to the entity by the individual or a third party may be inconsistent with other personal information held by the entity. For example, an identity document, letter, medical record or photograph
  - a court or tribunal has made a finding about the personal information, in a case involving the entity or in another case that comes to the entity's notice
  - the entity may be notified by another entity or person that the personal information is incorrect, or that similar personal information held by the other entity has been corrected

- a practice, procedure or system the entity has implemented in compliance with APP 1.2 (such as an auditing or monitoring program) indicates that personal information the entity holds requires correction.

APP13 Procedure

1. The Statutory Oversight Director will assign APP 13 requests to Statutory Oversight Officers.

2. Assigned officers are required to create a matter file in Trim.

    - Files are to be created under the APP12 and 13 Requests Mega Folder (MF) within SC15/89

    - Register the matter in the corresponding worksheet in the Privacy Matter register (financial year) located in Trim file 2014/593.

    - All correspondence is to be saved to file.

    File creation process is outlined at Annexure IV

3. Draft acknowledgement email to the applicant. Email should include:

    - Outline Corrections requested

    - The trim reference number assigned to the request

    - The timeframe for response

    - Name and contact details of the assigned officer

4. The email, addressed from Privacy@comcare.gov.au is then placed into the draft folder of the foi@comcare.go.au mailbox for AD QA. The email should BCC the assigned officer so that it can be saved to the matter file.

5. Email all business areas that may hold the information the applicant is requesting to be corrected. The email should include:

    - What corrections are being requested and by whom
    - A request for copies of the information
    - Folio, file and document numbers of all locations of the information
    - Any information the officer can provide in relation to the request or the information that is under the correction request
    - Provide five days for response

    Save email to Trim file.

6. Once response is received, save email and documents to Trim file. Assigned Officer will then review information taking into account the Grounds for correcting personal information outlined in the OAIC's APP guidelines.

Grounds for correcting personal information

The five grounds listed in APP 13 — 'accurate', 'up-to-date', 'complete', 'relevant' and 'not misleading' — are not defined in the Privacy Act. The first four terms are listed in APP 10.1, which deals with the quality of personal information that an APP entity can collect, use and disclose.

In applying the terms below to personal information, it is necessary to have regard to 'the purpose for which it is held'. Personal information may be incorrect having regard to one purpose for which it is held, but not another.

Accurate

Personal information is inaccurate if it contains an error or defect. An example is incorrect factual information about an individual's name, date of birth, residential address or current or former employment.

An opinion about an individual given by a third party is not inaccurate by reason only that the individual disagrees with that opinion or advice.

For APP 13 purposes, the opinion may be 'accurate' if it is presented as an opinion and not objective fact, it accurately records the view held by the third party, and is an informed assessment that takes into account competing facts and views.

Other matters to consider under APP 13, where there is disagreement with the soundness of an opinion, are whether the opinion is 'up-to-date', 'complete', 'not misleading' or 'relevant'. If an individual disagrees with an opinion that is otherwise not incorrect, the individual may associate a statement with the record of the opinion.

Up-to-date

Personal information is out-of-date if it contains facts, opinions or other information that is no longer current. An example is a statement that an individual lacks a particular qualification or accreditation that the individual has subsequently obtained.

Personal information about a past event may have been accurate at the time it was recorded, but has been overtaken by a later development. Whether that information is out-of-date will depend on the purpose for which it is held.

If current information is required for the particular purpose, the information will to that extent be out-of-date. By contrast, if information from a past point in time is required for the particular purpose, the information may not be out-of-date for that purpose

Complete

Personal information is incomplete if it presents a partial or misleading picture, rather than a true or full picture. An example, a statement that an individual has only two rather than three children will be incomplete under APP 13 if that information is held for the purpose of, and is relevant to, assessing a person's eligibility for a benefit or service.

Relevant

Personal information is irrelevant if it does not have a bearing upon or connection to the purpose for which the information is held.

Not misleading

Personal information is misleading if it conveys a meaning that is untrue or inaccurate or could lead a user, receiver or reader of the information into error. An example is a statement that is presented as a statement of fact but in truth is a record of the opinion of a third party. In some circumstances an opinion may be misleading if it fails to include information about the limited facts on which the opinion was based or the context or circumstances in which the opinion was first recorded.

A statement may also be misleading by failing to include other relevant information. An example is a statement that a dismissed employee was reinstated, without explaining that this followed the ruling of a court or tribunal that the dismissal was legally flawed.

Being satisfied

Where correction is requested by an individual and we require further information or explanation before we can be satisfied that personal information is incorrect, we should clearly explain to the individual what additional information or explanation is required and/or why we cannot act on the information already provided. We could also advise where additional material may be obtained. The individual should be given a reasonable opportunity to comment on the refusal or reluctance of the entity to make a correction without further information or explanation from the individual.

Where personal information is held for multiple purposes, we need only be satisfied that the personal information requires correction having regard to one of the purposes for which it is held, not all purposes.

Reasonable steps to correct

The guidelines tell us that a decision as to what constitutes ‘reasonable steps’ to correct personal information spans a range of options.

These include making appropriate additions, deletions or alterations to a record, or declining to correct personal information if it would be unreasonable to take such steps. In some instances it may be appropriate to destroy or de-identify the personal information (there are separate requirements to destroy or de-identify personal information in APPs 4 and 11 — see Chapters 4 and 11 respectively). The reasonable steps that Comcare should take will depend upon considerations that include:

- the sensitivity of the personal information. More rigorous steps may be required if the incorrect information is ‘sensitive information’ or other personal information of a sensitive nature.

- the possible adverse consequences for an individual if a correction is not made. More rigorous steps may be required as the risk of adversity increases.

- the practicability, including time and cost involved. However, we are excused from correcting personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

- the likelihood that we will use or disclose the personal information. For example, the likelihood of us using or disclosing the personal information may be relevant if it would be difficult or costly to make the correction requested by an individual.

- the purpose for which the personal information is held. Personal information may be held for multiple purposes, and require correction for one purpose but not for another purpose. Reasonable steps in these circumstances may require us to retain the original record of personal information for one purpose and create a record with the corrected personal information for another.

- record-keeping requirements that apply to the personal information under an Australian law or court/ tribunal order.

- whether the personal information is in the physical possession of the entity or a third party. For example, where personal information is in the physical possession of a third party, the entity may still 'hold' it and be required to take reasonable steps to correct it. In these circumstances, it may be a reasonable step for the entity to notify the third party that the information is incorrect and request that it be corrected. It will not generally be sufficient to refer the individual to the third party with physical possession. However, the third party with physical possession may also 'hold' the personal information, and if so, the individual will have a separate right to request the third party to correct it.

Special considerations apply to Commonwealth records. The term 'Commonwealth record' is defined in s 3 of the Archives Act. All records held by Comcare are considered 'Commonwealth Records'.

A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. Further, s 26 of the Archives Act makes it an offence to alter a Commonwealth record that is over 15 years old.

In relation to such records, and more generally, it may be reasonable (and consistent with statutory requirements) to:

- retain a version of a record which contains incorrect personal information

- associate a statement to clarify that, having regard to the purpose for which the personal information is held, the personal information is not accurate, up-to-date, complete, relevant or is misleading, and either including the correct personal information in the note or cross referencing where it is held (such as in an attachment to the record.

7. If the assigned officer is satisfied that there are grounds for correcting the Information the following should occur:

    a. Draft decision notice that includes:

        - Decision to correct information

        - Individuals right to request Comcare to notify another APP entity of a correction made to personal information that was previously provided to that other entity email. Provide timeframe of 14 days for such request.

    b. Officer should then make proposed correction to the information.

    c. Draft decision notice and document corrections should be sent to FOI@comcare.gov.au for Statutory Oversight AD QA.

    d. Once QA is finalised. Notify the business area who holds and uses the information of the decision and the corrections made.

e. To ensure Comcare still holds the original documentation (meeting requirements of the Archives Act 1988) save the corrected document over the top of the original in Trim.

f. Draft APP13 decision response email, attaching the decision notice and a copy of the corrected document. Ensure the From field is Privacy@comcare.gov.au. The email should BCC the assigned officer so that it can be saved to the matter file.

g. Place email into the draft folder of the foi@comcare.go.au mailbox for Statutory Oversight AD QA and Privacy check. The email will be sent by the AD.

h. If a request to notify other APP entities is received. The assigned officer should consider:
   - The sensitivity of the personal information. More rigorous steps may be required for or other personal information of a sensitive nature.
   - the possible adverse consequences for an individual if notice is not provided to the other entity. More rigorous steps may be required as the risk of adversity increases.
   - the nature or importance of the correction. For example, it may not be reasonable to provide notice of a small typographical error that does not materially affect the quality of the personal information.
   - the length of time that has elapsed since the personal information was disclosed to the other entity, and the likelihood that it is still being used or disclosed by the other entity
   - the materiality of the correction
   - the practicability of providing notice to another entity. For example, it may be impracticable to do so if the other entity has ceased carrying on business or has been substantially restructured.
   - the practicability, including time and cost of providing a notice to all entities to which the personal information was previously provided. However, an entity is not excused from giving notification by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.
   - Comcare is not required to provide notice of a correction if it would be impracticable or unlawful to do so. consider whether it would be practicable to notify some but not all of the other APP entities to which the entity previously disclosed the personal information. In these circumstances, the entity could discuss with the individual whether there are particular entities that they wish to be notified.

i. If notification is considered reasonable. Draft a notification email outlining the corrections made to the information. Place email into the drafts folder of FOI@comcare.gov.au for Statutory Oversight AD QA and Privacy check. The email will be sent by the AD.

j. Once the correction has been notified, the file can be closed. Please ensure:
   - All documents and correspondence is saved to the matter file in TRIM.
   - The APP13 request is finalised in the Privacy Matter register

8. If the Assigned Officer is not satisfied that there are grounds for refusal or is declining to correct the personal information, as the steps necessary to correct the personal information as requested are not reasonable in the circumstances. Draft a written notice that sets out:

- the reasons for the refusal, (except to the extent that it would be unreasonable to do so). The reasons for refusal should include (where applicable):
    - that the APP entity does not hold the personal information that the individual wishes to correct
    - that the entity is satisfied that the personal information it holds is accurate, up-to-date, complete, relevant and not misleading having regard to the purposes for which it is held, or
    - that the steps necessary to correct the personal information as requested are not reasonable in the circumstances
- the complaint mechanisms available to the individual (Comcare's feedback Team, followed by OAIC) and
- The individual should be advised of the right under APP 13.4 to request the Comcare to associate a statement with the personal information. Provide a timeframe for making such a request (14 Days).
- Consider also advising of the parallel right under the FOI Act to apply for a record to be amended or annotated, and of the right to Information Commissioner review of an adverse decision under that Act

NOTE: Comcare is not required to provide its reasons for refusing to correct personal information to the extent that it would be unreasonable to do so. This course should be adopted only in justifiable circumstances. An example would be where providing reasons would prejudice an investigation of unlawful activity, or prejudice enforcement action by an enforcement body.

9. Save draft decision notice to file. File naming convention is:
    - LAST NAME, Given name - Trim reference number – APP13 Notice
10. Send draft decision notice to FOI@comcare.gov.au for QA by Statutory Oversight AD.
11. At completion of QA, save finalised notice as PDF.
12. Draft response email, attaching decision notice letter and ensure the From field is Privacy@comcare.gov.au. The email should BCC the assigned officer so that it can be saved to the matter file.
13. Place email into the draft folder of the foi@comcare.go.au mailbox for AD QA and privacy check. The email will be sent by the AD.
14. If a request for associating a statement is received:
    a. We must take reasonable steps to associate the statement in a way that will make it apparent to users of the personal information. For example, a statement may be attached physically to a paper record, or by an electronic link to a digital record of personal information. The statement should be associated with all records containing personal information claimed to be incorrect.
        - For claim records it may be suitable to attaching the statement in a commitment comment - Liaise with the Claims Manager to have this completed.
    b. The content and length of any statement will depend on the circumstances, but it is not intended that the statement be unreasonably lengthy. A longer statement may be appropriate in some instances, such as where there is a large volume of personal information that the APP entity has refused to correct. If it is not practicable to attach an extensive statement to the personal information or otherwise create a link to the statement, a note could be included on, or attached to, the personal information referring to the statement and explaining where it can be found. Where we find it is not reasonable to associate an extensive statement to the personal

information, reasonable steps would generally include giving the individual an opportunity to revise the statement.

c. We must consider whether content in a statement may be irrelevant, defamatory, offensive, abusive or breach another individual's privacy — it may be unreasonable to associate a statement containing that content, however the individual should be given the option of revising the statement

15. Once the decision has been notified, a request to associate a statement has been actioned or the 14 day timeframe for a request for associating a statement has passed and any third party notifications have been considered an actioned, the file can be closed. Please ensure:
    - All documents and correspondence is saved to the matter file in TRIM.
    - The APP13 request is finalised in the Privacy Matter register

Office of the Australian Information Commissioner (OAIC)

Overview

The Office of the Australian Information Commissioner (OAIC) is an independent agency within the Attorney General's portfolio. Their primary functions are privacy, freedom of information and government information policy. Their responsibilities include conducting investigations, reviewing decisions, handling complaints, and providing guidance and advice.

Individuals can make complaints to the OAIC about the handling of their personal information. 'Handling of personal information' means to collect, use or disclose personal information. Generally, a complaint must be about a matter that occurred less than 12 months ago.

OAIC acts as an impartial third party when investigating and resolving complaints. They do not act for the applicant or the organisation or agency complained about.

Before they decide whether to investigate a complaint, they may make enquiries with Comcare (Early Resolution). In this situation, OAIC will write to Comcare and request initial information about the complaint. If the OAIC believe they can resolve the complaint during this process, they will attempt to do so.

There are situations that OAIC will not investigate complaints:

- The complaint doesn't involve personal information
- The applicant hasn't first complained to the organisation or agency they think has mishandled their personal information or they haven't had an opportunity to respond to the complaint
- The complaint is about something the applicant found out about more than 12 months ago

If OAIC decide to investigate a complaint involving Comcare, they will formally write to Comcare using the Privacy@comcare.gov.au address. The investigation officer will provide:

- A letter outlining the formal investigation under s 40(1) of the Privacy Act which will include:
    - a summary of the applicant's complaint
    - OAIC's initial view (applicable APP)

- Outcome being sought by applicant
- a request for response to the applicants proposed outcome and or information they require to assist in their assessment of the complaint.
- the contact name and number of the investigating officer
- a timeframe for response

Generally, the investigating Officer will try to discuss the issues raised in the complaint with the applicant and Comcare. OAIC's preference is to try to reach a mutual agreement on an outcome, rather than proceeding to a formal determination where the Information commissioner will decide what should happen.

If a mutual agreement regarding the complaint is reached the OAIC will close the complaint.

If the OAIC believes Comcare has proposed a reasonable outcome but the applicant is not happy with it, they may choose to close the complaint because we have adequately dealt with the matter, even though the applicant doesn't agree.

If OAIC is doesn't think the matter has been resolved or that Comcare hasn't adequately dealt with the matter, they will make a formal decision, called a determination, which states what the Comcare must do and is published on the OAIC website.

An applicant can choose to withdraw their complaint at any time without penalty

Possible outcomes for a complaint may be:

- taking steps to address the matter (such as being given access to personal information or having a record corrected)
- an apology
- a change to the practices or procedures
- training staff
- compensation for financial or non-financial loss
- other non-financial options (such as a complimentary subscription to a service)

In some situations, OAIC also accept an undertaking from Comcare to do, or stop doing, a specific thing so they don't breach the Privacy Act. If we fail to meet the undertaking, OAIC can ask a court to enforce it.

Where a breach of privacy is very serious, OAIC may seek a civil penalty. A civil penalty is like a fine and is not paid to the applicant.

Procedure

1. The Statutory Oversight Director will assign OAIC matters to Statutory Oversight Officers.
2. Assigned officers are required to create a matter file in Trim.

- Files are to be created under the OAIC Matters Mega Folder (MF) within SC15/89
- Register the matter in the corresponding worksheet in the Privacy Matter register (financial year) located in Trim file 2014/593.
- All correspondence is to be saved to file.

File creation process is outlined at Annexure IV

3. The Assigned Officer should locate and review the initial complaint/matter handled by Comcare
4. Draft response letter to OAIC. The letter should include:

    - The OAIC matter reference number
    - Comcare matter reference number
    - A summary of Comcare's position
    - A full background of Comcare's position, including
        - Background of complaint and our assessment
        - APP's we have considered and outline of our functions and activities
    - Comcare's response to applicants proposed outcome

5. Save draft response letter to trim. File naming convention is:

    - LAST NAME, Given name - Response to OAIC – OAIC Reference number - Trim reference number – Date

6. Send draft decision notice to FOI@comcare.gov.au for QA by Statutory Oversight AD.
7. At completion of QA, save finalised response letter as a PDF.
8. Draft response email, attaching response letter and ensure the from field is Privacy@comcare.gov.au. The email should BCC the assigned officer so that it can be saved to the matter file.
9. Place email into the draft folder of the foi@comcare.go.au mailbox for AD QA and privacy check. The email will be sent by the AD.

OAIC matters often take many months to reach conclusion, particularly where mutual agreement or conciliation is not successful.

The assigned Officer will be required to continue to liaise with OAIC on the matter and may be required to provide numerous responses to OAIC's investigation/assessment. Each response will need to be cleared by a Statutory Oversight AD. Follow steps above for QA and sending responses.

OAIC may request a teleconference to discuss the complaint and possible resolution. A Statutory Oversight AD or the Director must be involved in all teleconferences.

10. The Statutory Oversight Director should be briefed about the matter at each stage of correspondence and response.
11. If it is apparent that the matter is unable to be resolved through conciliation and it is likely to proceeds to determination by the Information Commissioner, The Statutory Oversight Director will need to brief Executive.
12. Once OAIC have made a determination or advise they are closing the matter. The assigned officer can finalise the matter in the Matter register and ensure all correspondence is saved to the Trim file.

Reporting

The Privacy Act does not impose any reporting requirements on agencies (other than reporting notifiable data breaches). Reporting notifiable data breaches is discussed under Privacy incidents at page 12.

The Statutory Oversight team provides statistics to Comcare's Executive operational meeting. This report includes:

- High Risk matters
- high profile matters
- statistics on internally reported Privacy incidents,
    - how many reported
    - how many finalised
    - how many were found to be an interference with Privacy
- Statistics on privacy complaints, APP12 and APP13 requests

Updates to Procedure Manual

This procedure manual must be updated in accordance with any legislative changes. The Statutory Oversight team monitors legislative changes through subscriptions to the Federal Register of Legislation.

The Assistant Director, Statutory Oversight, is responsible for updating the procedure manual

Australian Government

Comcare

FOI PROCEDURE MANUAL

Updated: May 2024

Contents

Key information

The Statutory Oversight team in the Legal Group is responsible for processing freedom of information (FOI) requests.

As there are strict timeframes around the processing of FOI requests, any new request received in any format must be forwarded directly to foi@comcare.gov.au for action.

What is Freedom of Information?

The *Freedom of Information Act 1982* (FOI Act) is legislation which provides members of the public with a right of access to documents held by Commonwealth Government agencies and ministers.

The FOI Act promotes government accountability and transparency by providing a legal framework for individuals to request access to government documents. This includes documents containing personal or other information, such as information about policy-making, administrative decision-making and government service delivery. Individuals can also request that ministers or agencies amend or annotate any information held about them.

Individuals have a right of access under the FOI Act to a document held by government unless the document:

- is held by an agency exempt from the FOI Act
- falls under one of the exemptions in the FOI Act
- falls under one of the conditional exemptions in the FOI Act, and releasing the document would be contrary to the public interest.

The FOI Act is also supplemented by the *Freedom of Information (Charges) Regulations 2019*, and the Guidelines issued by the Australian Information Commissioner (Information Commissioner Guidelines).

Service Expectations

You should endeavour to keep the Applicant informed across the life of the FOI process. Where an Applicant is exercising their right to request access to information, you must ensure you assist them and throughout the process, provide updates as necessary, including responding to queries promptly and providing updates to timeframes on decisions as required.

Purpose

The purpose of this Procedure Manual is to provide guidance for Comcare employees around the procedural steps for processing FOI requests.

The Procedure Manual must be read in conjunction with the FOI Act and the Information Commissioner Guidelines.

How does Comcare receive FOI requests?

Comcare receives FOI requests in a number of ways. The main ways are:

- Email: foi@comcare.gov.au or general.enquiries@comcare.gov.au
- Post: GPO Box 9905
  CANBERRA ACT 2601

Comcare may also receive a request as a transfer from another agency. These are usually received by email.

Overview of Comcare's FOI process

	Task	Responsible officer	Details
Day 1 – 14			
1.	Allocate	Director or Assistant Director	Review and allocate request to a Statutory Oversight Officer (**SOO**).
2.	Register	SOO	Create new HP TRIM file and record the matter in LEX.
3.	Review for validity	SOO	Determine whether request is valid. If invalid, advise applicant.
4.	Determine whether request should be transferred	SOO	Consider whether request should be transferred to another Commonwealth agency.
5.	Notify Business Areas (non-personal documents)	SOO	If the request is for non-personal documents, SOO should notify the General Manager of the relevant Business Area and Media of receipt of the request.
6.	Acknowledge request	SOO	Send acknowledgment letter within 14 days of receipt of the request.
7.	Determine whether to consult with applicant	SOO	Assess whether the request sufficiently identifies the documents sought or would require an unreasonable diversion of resources. Consult with applicant informally or formally.
8.	Send search/time estimate minute	SOO	Identify relevant Business Area which would hold requested documents.
9.	Retrieve documents	Business Area	Locate and send requested documents to SOO. Advise on any sensitivities in located documents.

	Task	Responsible officer	Details
			Advise SOO if large number of documents are located.
Day 15 – 19			
10.	Determine whether to consult with applicant	SOO	Assess whether processing the retrieved documents would require an unreasonable diversion of resources. Consult with applicant informally or formally.
11.	Consider processing charges	SOO	Consider whether to issue FOI processing charges.
12.	Determine whether to consult with third-parties	SOO	Review documents to identify third-parties (including other Commonwealth agencies). If necessary, consult with third-parties.
13.	Prepare decision	SOO	Prepare FOI decision and mark documents with redactions.
Day 20 – 30			
14.	Submit decision for quality assurance (QA)	SOO	Submit draft FOI decision and documents for QA via email to foi@comcare.gov.au.
		Assistant Director/Director	Review and provide feedback to SOO.
		SOO	Review QA feedback and make any necessary updates.
15.	Consult with Business Area	SOO	Provide documents proposed for release (i.e. with any relevant redactions applied) to Business Area for comment.
		Business Area	Confirm that there are no residual sensitivities in the documents proposed for release. For personal documents, EL1 level confirmation required. For non-personal documents, EL2 level confirmation required.

	Task	Responsible officer	Details
		SOO	For non-personal documents, notify relevant General Manager and Media Contact.
16.	Notify decision	SOO	Send final version of decision and documents to applicant.
Day 30 – 44			
17.	Update FOI disclosure log	SOO	If necessary, update FOI disclosure log within 10 days of notification of decision. Director of Statutory Oversight approval is required.
18.	Close record	SOO	Complete filing of documents in HP TRIM and update FOI Matter register.

Privacy considerations

Comcare takes its obligations under the *Privacy Act 1988* (Cth) very seriously. The SOO must be conscious of Comcare's privacy obligations during the entirety of the FOI decision-making lifecycle. This includes taking reasonable steps to confirm that any personal information used or disclosed is accurate, up-to-date, complete and relevant for the purposes for which it is being used or disclosed.

Process steps

Note: Refer to HP TRIM file MF18/639 for FOI templates and guides, and HP TRIM file SC15/90 for previous FOI matters and examples to consider. Always ensure to discuss matters with supervisors for any assistance.

1. Allocation

The Director or Assistant Director reviews a new request and allocates it to a Statutory Oversight Officer (**SOO**) by sending an email to the SOO.

Under Comcare's Freedom of Information Authorisations, decision-makers must be in the Statutory Oversight team and be at the APS 4 or above. The General Manager of Legal Group is also authorised to make FOI decisions.

The Director or Assistant Director may provide preliminary advice about how the request should be processed.

2. Registering requests

Once allocated, the SOO will register the request by:

- Creating a new file in HP TRIM:
  - Location: SC15/90

    - Naming convention: Freedom Of Information – [LAST NAME, First name] – summary of request. (E.g. “Freedom Of Information - DOE, Jane – investigation report into XYZ”).
- Record the matter in LEX.
- Saving a copy of the request into the newly created HP TRIM file.

3. Assess for validity

The SOO must assess the request to determine whether it is valid for the purposes of the FOI Act. Under section 15(2) of the FOI Act, valid request must be:

- in writing
- state that it is an application for the purposes of the FOI Act
- provide enough information about the requested document to reasonably identify it
- give details about how notices can be sent to the applicant (e.g., an email address or postal address).

Importantly, the applicant does not need to give any reasons why they are requesting the information.

If the request is not valid, the SOO must contact the applicant to advise them that the request is not valid and provide reasonable assistance to make it valid.

You should take a flexible approach to determining whether a request is valid, remembering the duty to assist the Applicant (ss 15(3b of the FOI Act)). Where a request is made and is missing minor details such as that it is for “the purposes of the FOI Act”, you should contact the Applicant and determine what they are seeking access to and whether access can be facilitated administratively noting Comcare’s broad statutory administrative access arrangements. Otherwise, you must assist them to make their request valid. Steps that may be necessary to assist an Applicant to make their request valid may include but are not limited to:

- Contacting the Applicant and determining what documents they seek
- Drafting the scope of a request and having the Applicant confirm the scope.

Staff requests

Under section 15A of the FOI Act, a current or former Comcare employee cannot request personnel documents relating to their employment unless they have first requested them through the People Team.

If the employee or former employee has not received a response from the People Team within 30 days or they are not satisfied with the outcome of their request from the People Team, then they can make an FOI request.

Accordingly, if a current or former Comcare employee makes an FOI request seeking personnel documents, they should be referred to helpdesk.payroll@comcare.gov.au at first instance.

4. Transfer to another agency

If the request is for documents more closely related to the functions of another agency, the SOO should consider transferring the request to the other agency under section 16 of the FOI Act.

This should occur in consultation with the possible receiving agency:

- at first instance, phone the agency to discuss the matter and enquire whether they would be willing to accept transfer of the request
- send the agency a formal email seeking confirmation that they accept transfer of the request
- contact the applicant in writing to advise the matter is being transferred
- email the receiving agency with a copy of the:
    - original request
    - the notice advising of transfer that was sent to the applicant.

Transfers should be actioned within 2 business days, as the accepting agency must still process the request based on the date the original agency received the request.

5. Notify Business Area

If the request is for non-personal documents (such as procedure manuals or policy documents), the SOO should send a courtesy email notification to the relevant General Manager (copying in their Executive Assistant) advising them of receipt of the request. On a case by case basis, the SOO may also need to be sent to the Office of the Chief Executive Officer.

A courtesy notification should also be sent to the Media Team.

These notifications should be sent within 2 business days of the request being allocated to the SOO.

6. Acknowledging the FOI request

The SOO must acknowledge the FOI request within 14 days of the day the request was received by Comcare (section 15(5)(a) of the FOI Act). However, the acknowledgment letter should be sent as early as possible.

The acknowledgement sets out the scope of the applicant's request, provides information on timeframes, and advises the applicant that, unless they contact otherwise, Comcare will consider Comcare staff details to be out of scope of the request.

7. Preliminary consultation with applicant

The SOO should review the scope of the request to determine whether preliminary informal consultations with the applicant should be undertaken. The purpose of the consultation is to efficiently assist the applicant to resolve issues with their request, as they may not be aware of the nature and volume of Comcare's records.

Examples where this may be appropriate include where, on the face of it, the request:

- captures a large number of documents
- is not clear.

Preliminary consultations can be made by phone or by email. If the applicant does not respond to the preliminary consultation within a reasonable period of time (e.g., 2 days), then the SOO should proceed with processing the request based on the original scope.

If the applicant agrees to revise the scope of their request, the SOO must confirm the revised scope in writing.

If the applicant does not engage with the preliminary consultation or if the consultation does not resolve the issues with the request, the SOO should:

- in the case where a large number of documents would be captured, proceed to Step 8 and request that the Business Area complete a time estimate minute
- in the case where the request is not clear, proceed immediately to Step 10.

8. Requesting documents

Note: If request does not provide sufficient information to identify the requested documents, proceed to Step 10.

Identification of Business Area

The SOO should identify the Business Area which would likely hold the requested documents. Common documents and Business Areas include:

Document	Business Area
Claims documents	Claims Management Group
Work Health and Safety Investigations	Regulatory Operations Group
AAT Documents	Claims and Litigation Services, Legal Group
Claims Manual and Guidance	Claims Management Group
Surveillance footage or reports	Fraud, Corporate Management Group

The SOO should use Comcare's Organisational Chart and intranet to help identify relevant Business Areas.

Once a Business Area has been identified, the SOO should contact an appropriate officer in the relevant team (e.g. an Assistant Director) by phone to discuss the request, advise on the FOI process, and obtain a positional email address for the SOO to send correspondence to.

Search email

The SOO should send an email to the Business Area providing:

- a copy of the request
- a search minute or time estimate minute as appropriate
- a timeframe for response (5 business days).

Search minutes and time estimate minutes

The SOO must determine whether to provide a search minute or a time estimate minute to the Business Area:

- **search minutes** provide information about steps taken by the Business Area to locate documents and to identify any sensitivities with the potential release of the documents.

They are used where the request identifies the documents and would not be unreasonable to process.
- **time estimate minutes** provide details about the number of documents, pages and possible sensitivities with the potential release of the documents. They are used where the request would likely capture a large number of documents and would require an unreasonable diversion of resources to process.

The SOO should determine which minute to send following preliminary discussions with the Business Area about the possible size and complexity of the request.

9. Retrieving documents

The Business Area is responsible for identifying and retrieving the requested documents. The Business Area should also ensure that it has completed the search minute to identify any sensitivities in releasing the documents. The Business Area does not need to describe their concerns with reference to the FOI Act.

It is important that search and time estimates are completed as they may be used to support Comcare's decisions in the course of an internal or external review.

Certification of searches

The Business Area must certify that they have taken all reasonable steps to locate the requested documents.

What constitutes 'all reasonable steps' to locate documents will depend on the terms of the request and may include searches of:

- Electronic records, including:
  - PRACSYS
  - HPE Trim
  - Emails
  - Shared drives
- Paper files.

Certification of searches should be completed at the EL1 level, and can be recorded electronically (such as by email) or by certifying the search minute.

Identifying sensitivities

Using the search minute, the Business Area must describe any sensitivities in the potential release of the documents located.

Whilst the Business Area does not need to describe their concerns with reference to the FOI Act, they should explain what harm, if any, could result in releasing information contained in the document.

Confirmation that sensitivities have been identified should be completed at the EL1 level, and can be recorded electronically (such as by email) or by certifying the search minute.

Large volume of documents identified

If a large number of documents are identified by the Business Area, the SOO should be contacted within 2 business days to discuss completing a time estimate minute and the possibility of consulting with the applicant to revise the scope of their request.

No documents found

If the Business Area does not locate the requested documents, the search minute should be completed setting out what steps were taken to locate the documents and advising why the documents could not be located or do not exist (e.g. “Comcare did not investigate that matter and therefore no inspection report exists”).

10. Formal consultation with applicant (Section 24AB of the FOI Act)

If the request is unclear or after the Business Area has provided a time estimate minute, the SOO must determine whether to undertake a formal consultation with the applicant under section 24AB of the FOI Act. A consultation is required where a ‘practical refusal reason’ exists in relation to the request.

A practical refusal reason exists where the request:

- does not provide sufficient information to identify the documents requested; or
- would require a substantial and unreasonable diversion of resources to process.

The purpose of the consultation is to assist the applicant to resolve issues with their request.

If the applicant has made multiple requests for the same document or documents, or the subject matter of the requests is substantially the same, the requests may be combined for the purposes of issuing a consultation under section 24AB of the FOI Act (section 24(2) of the FOI Act).

Where a consultation notice is issued under section 24AB of the FOI Act, the applicant must, within 14 days from the day after the notice is issued:

- revise the scope of their request
- refuse to revise the scope of their request, or
- withdraw their request.

Requirements of a consultation notice

A consultation must set out the following information (section 24AB(2) of the FOI Act):

- that the decision maker intends to refuse access to the request
- which practical refusal reason exists
- the name and contact details of the SOO (the SOO should not provide their direct phone number or email address)
- that the consultation period during which the applicant may consult the contact person is 14 days after the day the applicant is given the notice.

Timeframes

If the applicant does not revise or refuse to revise their request within the 14 day consultation period, then their request is taken to be withdrawn (section 24AB(7) of the FOI Act). If the applicant requires further time to revise their request, the consultation period may be extended with the applicant's agreement.

The consultation period, beginning from the day after the applicant is notified of the consultation and ending on the day the applicant revises or refuses to revise their request, is disregarded for the purposes of the processing timeframe (i.e. the 'processing clock' is paused during the consultation period).

Reasonable assistance

The SOO must provide the applicant with reasonable assistance to revise the scope of their request. Examples of reasonable assistance include:

- providing a breakdown or description of documents
- explaining Comcare's functions
- suggesting a scope of request that might be able to be processed
- suggesting other ways the applicant could revise their request (e.g. by specifying a specific timeframe, excluding draft document, etc.).

The SOO may need to contact the relevant Business Area to discuss the request and Comcare's operating environment so that the SOO can provide information and assistance to the applicant.

Cannot identify

A request must provide sufficient information as is reasonably necessary to enable a responsible officer of Comcare to identify the documents the applicant is seeking.

In determining whether the request provides sufficient detail, the SOO should read the request fairly and not take a pedantic approach to interpretation, recognising that applicants may not be aware of Comcare's operating environment.

Unreasonable diversion of resources

If the scope of the request captures a large number or significantly complex documents, the SOO should consider whether processing the request would require a substantial and unreasonable diversion of Comcare's resources.

In determining whether processing a request would be substantial and unreasonable, SOOs must consider the time that would be required:

- identifying, locating or collating documents
- examining the documents
- deciding whether to grant, refuse or defer access
- consulting with other parties
- redacting exempt material from the documents
- making copies of documents
- notifying an interim or final decision to the applicant.

SOOs should use the Charges Calculator to estimate the time that would be required to process the request in full. However, SOOs must amend the Charges Calculator to reflect the time that would be required to review and redact the documents, having regard to complexity of the documents under consideration. In general, the SOO will consider a range between 0.5 – 5 minutes to review and redact each page.

For example, it may be appropriate to allocate 0.5 minutes per page to review and redact each page for simple documents, such as letters previously sent to the applicant. For other material, such as investigation reports, material covered by legal professional privilege, or complex medical documents, it may be appropriate to allocate 3 minutes per page to review and redact each page.

Refusal to revise

If the applicant refuses to revise the scope of their request, the SOO should proceed to make a decision based on the scope of request that was used for the purposes of the consultation.

11. Charges

After receiving the documents from the Business Area, the SOO must consider whether to issue FOI processing charges under section 29 of the FOI Act and in accordance with the *Freedom of Information (Charges) Regulations 2019* (Charges Regulations).

FOI charges are discretionary and are used to recover some of the costs associated with processing the request. However, as a guiding principle in assessing costs, SOOs should consider the 'lowest reasonable cost' objective set out in section 3(4) of the FOI Act – that is, where the cost of calculating and collecting a charge might exceed the cost to Comcare in processing a request, it would generally be inappropriate to impose a charge.

Under the Charges Regulations, Comcare can impose a charge for the work already completed in relation to processing an FOI request or may charge based on an estimate of the work that would be required to process the request. In practice, Comcare will generally issue charges based on an estimate (which is then reviewed when the final decision is made).

You must refer to Comcare's FOI Charges Policy when considering whether to impose a charge.

Exceptions to charges

A charge cannot be imposed:

- for documents containing the applicant's own personal information
- where the request has not been processed within the statutory timeframe, including any relevant extensions.

Timeframes

Once notified of a preliminary assessment of charge, the applicant must respond in writing within 30 days either:

- agreeing to pay the charge (in full or the required deposit)
- contending that the charge:
    - has been wrongly assessed, or
    - should be reduced or not imposed, or

    - both
- withdrawing the request.

If no written response is received, the request is taken to have been withdrawn by operation of the FOI Act.

The period beginning from the day after the applicant is notified of the charge and ending on the day the applicant pays the charge (in full or the required deposit), is disregarded for the purposes of the processing timeframe (i.e. the 'processing clock' is paused during the consultation period).

Calculating a preliminary estimate of charge

Charges must be assessed in accordance with Part 1 or Part 2 to the Schedule 1 of the Charges Regulations, which contain tables showing the rates charged for each action undertaken whilst processing an FOI request.

Part 1 contains the rates for when a document is required to be produced to satisfy the request in accordance with section 17 of the FOI Act. When charging under Part 1, the SOO must obtain an estimate from the relevant Business Area of the actual costs associated with producing the document, calculated on a cost recovery basis.

Part 2 contains the rates for circumstances where documents have been located. The SOO estimates the time that would be required to process the request in full, taking into account time required for searching and retrieving the documents, reviewing the documents, applying any redactions, and writing a decision. SOOs should use the Charges Calculator to assist them in estimating the relevant charge. However, SOOs must amend the Charges Calculator to more accurately reflect the time that would be required to review and redact the documents, having regard to complexity of the documents under consideration.

Comcare cannot charge for the first 5 hours of decision-making time, accordingly this time must be disregarded for the purposes of the calculating charge.

Reconsideration of charges

The SOO must provide a reconsideration of charge decision within 30 days of the day after an applicant responds to the preliminary assessment in writing contending that:

- the charge has been wrongly assessed
- should be reduce or not imposed, or
- both.

A reconsideration of charge decision requires that the SOO review the preliminary assessment of charge. In addition to any matters raised by the applicant, the SOO must consider (section 29(5) of the FOI Act):

- whether giving access to the documents in the general public interest or in the interest of a substantial section of the public
- whether paying the charge would cause the applicant financial hardship.

The public interest test in relation to a charges reconsideration requires the SOO to consider whether the general public interest, or in the interests of a substantial section of the public, in relation to the hypothetical release of documents (that is, if the documents were released in full)

and whether it outweighs the assessed charge. Relevant public interest considerations could include whether the documents relate to a matter of public debate or significant public spending.

If the applicant contends that paying a charge would cause them financial hardship, they can be expected to provide evidence of that hardship. Relevant evidence could include evidence that the applicant receives a pension or income support payment or other evidence about their financial circumstances.

For the purposes of FOI charges, financial hardship is defined as where payment of the charge would leave the applicant unable to provide food, accommodation, clothing, medical treatment, education or other necessities for themselves or their family, or other people for whom they are responsible.

12. Third party Consultations

Where a document within scope of the request contains material relating to a third party, the SOO should consider whether it is appropriate to undertake a consultation.

Consultations may be undertaken where the documents contain material obtained from or relating to:

- other Commonwealth agencies (courtesy consultations)
- businesses or other organisations (section 27 of the FOI Act)
- persons other than the applicant (section 27A of the FOI Act)
- State agencies (section 26A of the FOI Act).

Consultations provide the third party with an opportunity to comment on the potential release of the documents under the FOI Act. The third-party may provide further information to the SOO to assist in making a decision about the release of documents.

Importantly, whilst the SOO must consider any submissions provided by a third party, the final decision about the release of the documents rests with the SOO.

Where the SOO decides to release documents where a third party (other than other Commonwealth agencies) has contended that they should be exempt from release, the third party will retain internal and external review rights in relation to Comcare's decision. This means that the documents that the third party objected to cannot be released until the third party's review rights have expired (including internal review and external review rights).

General information

When engaging in a consultation, SOOs must be mindful of not disclosing the identity of the applicant unless they have consented the disclosure of their personal information. SOOs may consider asking the applicant for their consent to disclose their identity.

SOOs must also ensure that they do not provide the third party with information that is not relevant to the consultation. The SOO may be required to prepare a new copy of the document for the purposes of the consultation with irrelevant material redacted.

Commonwealth agencies

The SOO should consult with another Commonwealth agency's FOI Team where the requested documents contain material that originated from or relates to that agency.

Any consultation with another agency does not add additional processing time.

As a courtesy, the SOO should advise the consulted agency of the outcome of their decision on the release of documents, particularly in circumstances where the SOO has made a decision contrary to the agency's submissions.

Documents containing business information

Where a request captures a document containing business information of a third party and the third party would reasonably wish to contend that the information is exempt from release, the SOO must provide the third party with an opportunity to provide submissions about the release of the information.

The relevant third party may contend that the information is exempt under:

- section 47 of the FOI Act – the information is a trade secret or other commercially valuable information
- section 47G of the FOI Act – release of the information would, or could reasonably be expected to, unreasonably affect the business in respect of their lawful business, commercial or financial affairs or prejudice the future supply of information to the Commonwealth.

In determining whether the third party would reasonably wish to contend that the information is exempt, the SOO must consider:

- the extent to which the information is well known
- whether the business is known to be associated with the matters dealt with in the information
- the availability of the information from publicly accessible sources
- any other matters the SOO considers relevant.

A consultation in relation to business information, under section 27 of the FOI Act, adds 30 days to the processing time.

Documents containing personal information

Where a request captures a document containing personal information of a third party and the third party would reasonably wish to contend that the information is exempt from release, the SOO must provide the third party with an opportunity to provide submissions about the release of the information.

The relevant third party may contend that the information is exempt under section 47F of the FOI Act – release of the material would be an unreasonable disclosure of their personal information.

In determining whether the third party would reasonably wish to contend that the information is exempt, the SOO must consider:

- the extent to which the information is well known
- whether the person is known to be associated with the matters dealt with in the information
- the availability of the information from publicly accessible sources
- any other matters the SOO considers relevant.

A consultation in relation to personal information, under section 27A of the FOI Act, adds 30 days to the processing time.

Documents containing information obtained from a State

Where a request captures a document containing information that originated with, or was received from, a State or authority of the State, the SOO must provide the State or authority of the State an opportunity to provide submissions about the release of the information.

Before commencing a consultation, the SOO must be satisfied that arrangements exist between the Commonwealth and the State regarding consultations under the FOI Act. The SOO should contact the relevant State authority FOI Team to discuss the arrangements.

The relevant State may contend that the information is exempt under section 47B of the FOI Act, where disclosure:

- would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a State
- would divulge information or matter communicated in confidence by or on behalf of the Government of a State or an authority of a State, to the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth
- would divulge information or matter communicated in confidence by or on behalf of an authority of Norfolk Island, to the Government of the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth
- would divulge information or matter communicated in confidence by or on behalf of the Government of a State or an authority of a State, to an authority of Norfolk Island or to a person receiving the communication on behalf of an authority of Norfolk Island

A consultation in relation to information obtained from a State, under section 26A of the FOI Act, adds 30 days to the processing time.

13. Making a decision

Once the SOO has obtained the documents, received any applicable processing charges, and considered any consultation responses, they must make a decision about the release of the documents. The SOO must give a person access to a document unless it is:

- an exempt document, or
- a conditionally exempt document and release would be contrary to the public interest.

If the SOO determines that parts of the document are exempt, they must consider whether it possible to prepare an edited copy of the document with the exempt material redacted.

In cases where a practical refusal reason exists or the requested document could not be located or does not exist, the SOO will make a decision without reviewing a document.

Common types of information held by Comcare

Type of information	Decision-maker should consider…
Third-party personal information	Section 47F of the FOI Act

Type of information	Decision-maker should consider…
Third-party business information	Section 47G of the FOI Act
Draft documents	Section 47C of the FOI Act
Opinions or recommendations	Section 47C of the FOI Act
Medical information that, if released, may harm the applicant	Section 47F of the FOI Act
Details of investigations	Section 37 of the FOI Act Section 47E(d) of the FOI Act
Witness statements	Section 37 of the FOI Act Section 47F of the FOI Act
Information obtained in confidence	Section 45 of the FOI Act
Legal advice or requests for legal advice	Section 42 of the FOI Act
Information obtained from other agencies	Section 47E(d) of the FOI Act
Information describing detailed Comcare processes	Section 47E(d) of the FOI Act
Details of staff management action	Section 47E(c) of the FOI Act
Comcare employee details (names, direct phone numbers, email addresses)	Section 47E(d) of the FOI Act Section 47F of the FOI Act
Out of scope or irrelevant material	Section 22 of the FOI Act

Exemptions

Exempt documents in Division 2 of Part IV of the FOI Act which are relevant to Comcare include:

- documents affecting enforcement of law and protection of public safety (section 37 of the FOI Act)
- documents subject to legal professional privilege (section 42 of the FOI Act)
- documents containing material obtained in confidence (section 45 of the FOI Act)
- documents disclosing trade secrets or commercially valuable information (section 47 of the FOI Act).

The exemptions in Division 2 of Part IV of the FOI Act are not subject to an overriding public interest test. In other words, if a document meets the criteria to establish a particular exemption, it is exempt. There is no additional obligation to weigh competing public interests to determine if the document should be released.

Conditional exemptions

Conditionally exempt documents in Division 3 of Part IV of the FOI Act which are relevant to Comcare include:

- Commonwealth-State relations (section 47B of the FOI Act)
- deliberative processes (section 47C of the FOI Act)
- certain operations of agencies (section 47E of the FOI Act)
- personal privacy (section 47F of the FOI Act)
- business (other than documents to which section 47 of the FOI Act applies) (section 47G of the FOI Act).

Where a document is conditionally exempt, the SOO must grant access to the document unless giving access would, on balance, be contrary to the public interest.

In considering the public interest, the SOO must weigh the factors favouring access to the documents against the factors against providing access to the document. Section 11B(3) of the FOI Act sets out four factors which favour access to documents and must be considered if relevant. These factors are whether disclosure would:

- promote the objects of the Act
- inform debate on a matter of public importance
- promote effective oversight of public expenditure
- allow a person to access his or her personal information.

Section 11B(4) of FOI Act also sets out factors that must not be taken into account when weighing the public interest. The irrelevant factors are whether:

- access to the document could result in embarrassment to the Commonwealth Government, or cause a loss of confidence in the Commonwealth Government
- access to the document could result in any person misinterpreting or misunderstanding the document
- the author of the document was (or is) of high seniority in the agency which the request for access to the document was made
- access to the document could result in confusion or unnecessary debate.

It is not sufficient to list the factors considered, the SOO must weigh the factors and come to a conclusion about where the public interest lies in a particular matter.

Practical refusal reasons

A request should be refused where a practical refusal reason continues to exist following a consultation processes under section 24AB of the FOI Act (see Step 9 for information regarding consultations under section 24AB of the FOI Act).

A practical refusal reason will exist if following a consultation process under section 24AB of the FOI Act, the request:

- does not provide sufficient information as is reasonably necessary to enable a responsible officer of Comcare to identify the documents the applicant is seeking, or
- would require a substantial and unreasonable diversion of resources to process.

Where an SOO refuses a request on the basis that the processing a request would require a substantial and unreasonable diversion of resources, the SOO must obtain a representative sample of approximately 10% of the documents that are captured by the scope of the request. The SOO should obtain the sample of documents from the relevant Business Area.

Documents do not exist or cannot be found

The SOO may refuse access to a document if they are satisfied that all reasonable steps have been taken to locate the document and they are satisfied that the document cannot be found or does not exist.

The SOO relies on the Business Area to confirm what searches were conducted and to advise on the reasons why the document cannot be located or does not exist. An explanation of the searches undertaken and any reasons for why the document could not be located should be included in the decision letter sent to the applicant.

In determining whether all reasonable steps have been taken to locate the documents, the SOO should consider:

- the subject matter of the documents
- the normal arrangements for processing and storage of the documents
- any information to establish the existence of the document
- the age of the documents.

Writing a decision

Section 26 of the FOI Act sets out the formal requirements of an FOI decision letter. The SOO must prepare a decision letter which explains to the applicant:

- what exemptions were applied to documents (if any)
- the reasons why those exemptions were applied (including relevant public interest considerations)
- what the applicant's review rights are.

In addition, if the applicant paid a processing charge, the SOO must make a decision fixing the charge based on the actual time taken to process the request. If the actual time taken to process the request is less than the estimated time, the SOO must refund the difference in the charge. However, if the actual processing time is greater than the estimated time, no additional charge can be levied against the applicant.

SOOs should use the templates available as a base for their decision letters, however the templates must be amended to reflect the particular circumstances of the request.

Preparing documents

The SOO should combine all relevant documents into a single PDF document and add a header and page numbers to the document. The header should be in the format "FOI: 2024/XXXX", which indicates from where the applicant obtained the documents.

Exemptions applied to the document should be marked using the redaction function in Adobe Pro and must use overlay text showing the relevant exemption applied to the material.

14. QA

All formal letters (including section 24AB consultations and decision letters) and documents processed under the FOI Act must be quality assured (QA) by an Assistant Director or the Director of the Statutory Oversight Team.

The SOO must refer the letter or document for QA by sending a QA referral template email to FOI@comcare.gov.au.

A decision should be submitted for QA at least 10 business days prior to the due date.

The QAer may provide feedback and refer the letter or document back to the SOO for further action.

15. Business Area notification

After QA, the SOO must provide the relevant Business Area with a copy of the documents in the form proposed for release with any relevant redactions applied (i.e. in the form proposed to be provided to the applicant), and seek the Business Area's advice as to whether there are any residual sensitivities with the release of the document.

The SOO should provide the Business Area with 5 business days for their response.

Personal documents

Where the requested documents are documents containing the applicant's personal information (such as material from their compensation claim file), EL1 certification is sufficient.

Non-personal documents

Where the requested documents are documents that do not contain the applicant's personal information (such as Comcare policy documents), EL2 certification is required.

Once EL2 certification is received, the SOO must also notify, 5 business days prior to issuing the decision:

- the Business Area's General Manager
- the Media Adviser
- if the documents relate to significant issue, the Office of the CEO.

16. Notifying the decision

Following Business Area notifications, the SOO must send the decision letter, together with any relevant documents, to the applicant. The decision letter must be provided to the applicant prior to the due date.

Prior to releasing the decision and documents to the applicant, the SOO must:

- convert and save the decision letter in a PDF format
- ensure that redactions have been correctly applied to documents for release
- remove metadata from the documents before release
- ensure that third-party documents will not be released until the third-party's review rights expire.

The SOO should send a courtesy email to the relevant Business Area within 5 business days of notifying the applicant, to advise that the matter has been completed and that no further action is required from them.

If a decision due date falls on a weekend or public holiday, then the decision can be notified on the following business day.

17. Disclosure Log

Following release of a document under the FOI Act, the SOO must consider whether the document is required to be published on Comcare's FOI Disclosure Log.

Section 11C of the FOI Act requires that documents released under the FOI Act be published on the agency's disclosure log, except if the document contains:

- personal information about any person, if it would be unreasonable to publish the information
- information about the business, commercial, financial or professional affairs of any person, if it would be unreasonable to publish the information.

Documents must be published on the Disclosure Log within 10 days business days after the person is given access to the document.

Where the SOO determines that a document should be published on the Disclosure Log, they must:

- complete a Disclosure Log Determination, to be cleared by the Director of the Statutory Oversight Team
- email Communications@comcare.gov.au with a request that the Comcare's Disclosure Log website page be updated with the details of the relevant document.

18. Finalising the matter

Following notification of the decision letter and documents and, if relevant, updates to the Disclosure Log are made, the SOO must finalise the FOI matter.

To finalise the matter, the SOO must:

- File all documents (including draft letters and marked up versions of decision documents) and correspondence in the relevant TRIM folder
- Update LEX with all relevant information to reflect the outcome of the request.

FOI timeframes

An FOI request must be processed within 30 calendar days from the day after it is received (section 15(5)(b) of the FOI Act).

The processing timeframe is extended in certain circumstances, including:

- by written agreement with the applicant (section 15AA of the FOI Act)
- by agreement of the Information Commissioner where the request is complex or voluminous (section 15AB of the FOI Act)

- for consultations under sections 26A, 27 and 27A of the FOI Act with third parties (sections 15(6) and 15(7) of the FOI Act)

The processing timeframe is disregarded during:

- consultations with the applicant under section 24AB of the FOI Act
- the period between the applicant being notified of a charge under section 29 of the FOI Act and the charge or deposit being paid by the applicant.

If a decision is not made within the processing timeframe, the request is considered to have been refused by the principal officer of the agency. The SOO should still proceed to issue a decision, however, an internal review will not be available to the applicant.

Section 15AA

The SOO may wish to consider seeking an extension with the agreement of the applicant under section 15AA. The request for extension can be up to 30 days, as either a single extension or a series of shorter extensions. This may be in addition to any time extensions that apply for third party consultation. The SOO must seek written agreement of the applicant. In order for the extension to be valid, the SOO must give written notice of the extension to the Information Commissioner as soon as practicable (within 1 business day) through OAIC's online form. This must be completed before the expiration of the processing period.

Section 15AB

The SOO can apply to the Information Commissioner for an extension of time under section 15AB. The request must explain why the applicant's request is complex or voluminous. The SOO must include the scope of the request and the range of documents covered, work already undertaken on the request, any consultation with the applicant concerning length of time, and measures taken to ensure a decision is made within the extended time period, and to keep the applicant informed about progress. The Information Commissioner may share your submission with the applicant.

The SOO should only seek an extension of time under s 15AB after they first obtained, or attempted to obtain, the applicant's agreement for an extension under s 15AA. The application must be made before the expiration of the processing period. Applications must be made through OAIC's online form.

Communication with applicants

There is an expectation of clear communication with Applicants regarding timeframes, particularly in circumstance where the timeframe varies on multiple occasions. Where the timeframe for the notification of a decision changes from the original due date the Applicant should be notified of the change, why the change has occurred (i.e. what mechanism under the FOI Act extended the timeframe) and the new due date. This should occur as soon as practicable either at the time an extension is notified or within 2 business days after it has been agreed.

Review of FOI Decisions

An applicant or an affected third party can seek internal and external review of FOI decisions made by Comcare. Applicants and affected third parties can seek review of:

- a decision refusing to give access to a document in accordance with a request

- a decision giving access to a document but not giving access to all documents to which the request relates
- a decision purporting to give, in accordance with a request, access to all documents to which the request relates, but not actually giving that access
- a decision under s 29 relating to imposition of a charge or the amount of a charge
- a decision to give access to a document to a qualified person under s 47F(5)

Internal Reviews

A request for internal review must be made within 30 days from the date the applicant receives the original decision.

An internal review decision must be made by a decision maker other than the original decision maker and will generally be a more senior member of the Statutory Oversight Team.

The internal review decision maker will consider the request afresh, taking into account submissions made by the applicant. If necessary, the decision maker may conduct fresh searches for documents or may rely on the documents already retrieved.

Information Commissioner Reviews

An applicant or affected third party may seek Information Commissioner review of Comcare's decisions and the applicant does not need to have first sought internal review of the decision.

The applicant or affected third party must notify the Office of the Australian Information Commissioner (OAIC) of their request for Information Commissioner review within 60 days of receiving the reviewable decision.

An Information Commissioner review is a merits-based review and is non-adversarial. The OAIC will ask Comcare to provide relevant documents together with submissions in support of its decision.

The Information Commissioner can make a decision to:

- not review the matter
- affirm Comcare's decision, or
- vary Comcare's decision.

During the Information Commissioner review process, Comcare may:

- enter into an agreement with the applicant, under section 55F of the FOI Act, to process a new request and finalise the Information Commissioner review, or
- issue a decision under section 55G of the FOI Act, granting access to a document under review.

Administrative Appeals Tribunal Reviews

If an applicant, affected third party, or agency is not satisfied with the decision made by the Information Commissioner, they can seek a review of the decision by the Administrative Appeals Tribunal (AAT).

The applicant, affected third party, or agency must lodge their application for AAT review within 28 days after the day of receiving the Information Commissioner's decision.

Updates to Procedure Manual

This procedure manual must be updated in accordance with any legislative changes. The Statutory Oversight team monitors legislative changes through subscriptions to the Federal Register of Legislation.

The Assistant Director, Statutory Oversight, is responsible for updating the procedure manual.

Australian Government

Comcare

FREEDOM OF INFORMATION CHARGES POLICY

Finalised April 2024

Contents

Purpose

1. This document details Comcare's policy on charging for the release of documents requested under the *Freedom of Information Act 1982* (**FOI Act**).

Scope

2. Comcare's Charge Policy is consistent with the FOI Act, the *Freedom of Information (Charges) Regulations 2019* (**Charges Regulations**), and Part 4 of the guidelines issued by the Australian Information Commissioner under section 93A of the FOI Act (**Guidelines**).

Background

3. Comcare may impose a charge in respect of a request for access to a document or for providing access to a document, under section 29 of the FOI Act. The charge must be assessed in accordance with the Charges Regulations.

4. The Information Commissioner has published guidance and advice that helps decision makers identify the steps in calculating a charge.

5. Decision on the application of charges will be made by the authorised decision maker processing the request in consultation with their supervisor.

Guiding principles

6. The amount of any charge imposed should be:
    a. determined bearing the objects of the FOI Act in mind
    b. reasonable, taking into account all relevant factors
    c. proportionate to the cost of making a decision and providing access, as well as any general public interest supporting release of the requested documents (see section 29(5)(b) of the FOI Act).

7. Where the cost of calculating and collecting a charge might exceed the cost to Comcare to process the request, it may generally be more appropriate not to impose a charge.

8. The objects of the FOI Act provide the basis for the following principles relevant to charges under the FOI Act:
    a. A charge must not be used to unnecessarily delay access or to discourage an applicant from exercising the right of access conferred by the FOI Act.
    b. A charge should fairly reflect the work involved in providing access to documents.
    c. Charges are discretionary and should be justified on a case by case basis.
    d. A decision to impose a charge should be transparent.

Opportunities to obtain access outside the FOI Act

9. If an applicant requests claim related information, you could seek their confirmation to process their request as a section 59 request (under the *Safety, Rehabilitation and Compensation Act 1988*) instead of the FOI Act. You must ensure that they also withdraw their FOI request, or you will still be required to process it under the FOI Act.

10. There is a range of Comcare reports and operational documents on Comcare's Information Publication Scheme, including Comcare's Claims Manual.

11. There are also some documents accessible on Comcare's Freedom of information Disclosure Log from previous FOI requests already processed by Comcare.

When to consider imposing a charge

12. It is up to the authorised decision maker's discretion to impose a charge, however you should consult with your supervisor early if you are considering to impose a charge. It may be appropriate to impose a FOI charge where:
    a. the applicant has requested access to a substantial volume of documents and significant work will be required to process the request
    b. the documents are primarily of interest only to the applicant and are not of general public interest or of interest to a substantial section of the public
    c. the information in the documents has already been published by Comcare and the documents do not add to the public record
    d. the applicant can be expected to derive a commercial or personal benefit or advantage from being given access and it is reasonable to expect the applicant to meet all or part of the charge.

Charges that cannot be imposed

13. There is no application fee for a FOI request.

14. Comcare cannot impose a charge:
    a. for giving access to an individual's own personal information (s 7(1) of the Charges Regulations)
    b. if it fails to make a decision on the request within the statutory processing period – the statutory period includes any extensions of time under ss 15(6), 15(8), 15AA and 15AB, but not s 15AC of the FOI Act (ss 7(2) and (3) of the Charges Regulations); Comcare must refund any deposit paid in these circumstances (s 12(3)(b) of the Charges Regulations)
    c. for making an internal review decision.

15. An FOI request cannot be 'split' into parts. Therefore, an applicant cannot be found liable to pay a charge for a portion or part of a request. A charge can only be imposed on the request as a whole.

Charges that may be imposed

16. The charges that may be imposed by Comcare with respect to a request for access to a document are specified in Schedule 1 of the Charges Regulations. While the decision to impose a charge is discretionary, calculation of the charge must be in accordance with the amounts specified in Schedule 1 of the Charges Regulations. Part 1 of Schedule 1 specifies charges related to making a decision on a request and Part 2 specifies charges for giving access to a document.

17. The most common charges are:

Activity item	Charge
Search and retrieval: time spent searching for or retrieving a document	$15 per hour
Decision making: time spent deciding to grant or refuse a request, including examining documents, consulting other parties, making deletions, or notifying any interim or final decision on the request	First five hours: Nil Subsequent hours: $20 per hour
Photocopy: a photocopy of a written document	$0.10 per page
Other copies: a copy of a written document other than a photocopy	$4.40 per page
Inspection: supervision by an officer of an applicant's inspection of documents or the hearing or viewing of an audio or visual recording	$6.25 per half hour (or part thereof)
Delivery: posting or delivering a copy of a document at the applicant's request	Cost of postage or delivery

18. The Charges Regulations set out an hourly rate that applies regardless of the classification or designation of the officer who undertakes the work. The Charges Regulations do not specify a method for charging for part of an hour of search or retrieval or decision-making time. If such a charge is to be imposed, it should be calculated on a proportionate basis, for example, 30 minutes work should be charged at 50 percent of the hourly rate.

Estimating a charge

19. Comcare should undertake a preliminary assessment of the charge. The preliminary assessment can be the work already done by Comcare (search and retrieval for documents) or an estimated charge for the work still to be done (examination of documents, drafting the decision).

20. An estimated charge must be as fair and accurate as possible. Comcare recommends obtaining an estimate of the processing time by sampling at least 10% of the documents at issue.

21. Please ensure to use the Charges Calculator on Content Manager when undertaking a preliminary assessment of the charge. This should be provided to your supervisor for

consideration along with the draft notice to the applicant before imposing the charge on the applicant. It is important to keep records on your preliminary assessment of charges.

Notifying a charge

22. An applicant must be given written notice when Comcare decides the applicant is liable to pay a charge. The notice must specify:
    a. that the applicant is liable to pay a charge
    b. Comcare's preliminary assessment of the charge and the basis for the calculation
    c. the applicant's right to contend that the charge has been wrongly assessed or should be reduced or not imposed
    d. in considering any contention, Comcare must take into account whether payment of the charge would cause financial hardship to the applicant or the person on whose behalf the application was made, and whether giving access to the document would be in the public interest
    e. the amount of any deposit payable by the applicant (see s 12(1) of the Charges Regulations)
    f. the applicant's obligation to notify in writing within 30 days that they:
        i. agree to pay the charge
        ii. dispute the charge, including seeking waiver or reduction, or
        iii. withdraw the FOI request
    g. that the FOI request will be taken to have been withdrawn if the applicant fails to respond within 30 days.

Reduction or waiver of charges

23. If an applicant contends that a charge should be reduced or waived, Comcare must consider:
    a. whether payment of the charge, or part of it, would cause financial hardship to the applicant or to a person on whose behalf the application was made, and
    b. whether giving access to the document in question is in the general public interest or in the interest of a substantial section of the public (see section 29(5) of the FOI Act).

Deposits

24. Comcare may require the applicant to pay a deposit (section 29(1)(e) of the FOI Act, section 12(1) of the Charges Regulations). The deposit cannot be higher than $20 if the notified charge is between $25 and $100, or 25 percent of a notified charge that exceeds $100 (section 12(2) of the Charges Regulations). However, please keep in mind that where the cost of calculating and collecting a charge might exceed the cost to Comcare to process the request, it may generally be more appropriate not to impose a charge.

25. A deposit paid must be refunded to the applicant if Comcare fails to make a decision on the applicant's FOI request within the statutory time limit or sets a final charge after making a decision on the FOI request, that is lower than the amount already paid as a deposit (s 10(5)(a) of the Charges Regulations).

Collecting the remainder of a charge

26. If an applicant is liable to pay a charge, the charge must be paid before access to documents can be given (section 11A(1)(b) of the FOI Act and section 11(1) of the Charges Regulations).

27. The FOI Act does not set a time limit for an applicant to pay the remaining balance of a charge after a decision is made on the FOI request. If the applicant does not pay the charge, the requested documents cannot be released and there is no mechanism in the FOI Act to finalise the request.

28. Comcare should advise the applicant that if they do not receive the remaining balance within 60 days, the FOI request will be taken to have been withdrawn.

Correction of final charge

29. After making a decision on an FOI request where a charge was estimated under section 9 of the Charges Regulations, Comcare is required to calculate the final charge based on the actual time taken to process the request. Comcare recommends using the Charges Calculator here as well.

30. The new charge may be different to the estimated charge. If the new charge is less than the amount already paid by an applicant, a refund of the difference must be made (section 10(5)(a) the Charges Regulations). If the new charge is higher than the amount already paid, that payment will be treated as a deposit on account of the charge (s 10(5)(b)).

ESTIMATE

FOI CHARGES ESTIMATE (NOV 2010)		
(insert data in shaded boxes only)		
BASIC DATA ESTIMATE		
Number of relevant files		
Number of relevant pages		
Number of relevant documents		
Number of fully exempt pages		
Number of pages released with deletions		
Number of documents for access via inspection		
Percentage of request relating to applicant's own personal information		
Number of third parties to consult		
PROCESS - search and retrieval	**TIME (in hours)**	**COST @ $15 per hr**
Search and retrieval (10 mins per file)	0.00	$0.00
Search files and tag relevant pages (45 mins average per file)	0.00	$0.00
preparing schedules detailing all relevant documents (basic data entry e.g. doc no, date, description - 30 minutes per 10 documents)	0.00	$0.00
Search & Retrieval Subtotal	0.00	**$0.00**
PROCESS - decision-making	**TIME (in hours)**	**COST @ $20 per hr**
examine relevant pages for decision making (5 mins per relevant page).	0.00	$0.00
exempted pages (5 mins extra per page to cover additional consideration of complexity of material, elements of exemption claim, public interest etc).	0.00	$0.00
pages released with deletions (5 mins extra per page to cover time needed to redact the material)	0.00	$0.00
consult third parties (2 hours per third party)	0.00	$0.00
preparation and notification of decision (3 hours for statement of reasons, plus 4 hours per 250 relevant pages to complete schedule to record decision) - NB if several exemptions are involved, further time may be required.	3.00	$60.00
Decision-making Subtotal (before deduction of 5 hours)	3.00	$60.00
Decision-making Subtotal (after deduction of first 5 hours free for all)	0.00	**0**
ACCESS - view / inspect	**TIME (in hours)**	**COST @ $6.25 per 1/2 hr**
Access given through inspection of documents (10 min per document, rounded up to nearest 1/2 hour)	0.00	0.00
Access given through hearing and/or viewing of documents e.g audio/visual material - insert duration of files and add 1/2 hour set-up and pack-up time (rounded up to nearest 1/2 hour)		0.00
Inspection/Viewing Subtotal	0.00	**$0.00**
ACCESS - copy and post	**PAGES**	**COST @ 10c a page**
Photocopies of estimated released docs (including those with deletions)	0	**$0.00**
Packaging and postage-insert estimated cost	N/A	
Photocopying & Postage Subtotal		**$0.00**
ESTIMATED TOTALS		
NUMBER OF RELEASED PAGES		**0**
TIME (in hours)		**0.00**
TOTAL COST		**$0.00**
Financial hardship/public interest discount		**$0.00**
TOTAL COST (after discount)		**$0.00**
DEPOSIT REQUIRED		**N/A**
USING THIS TOOL		
based on a number of assumptions which are described in column A. The appropriateness of those assumptions to the particular circumstances should be tested on each occasion - for example, repetitious material can be dealt with more quickly, as can publicly available documents. If the decision is to release everything in full, the time for notifying the decision should be reduced significantly.		

Number of agency's files that contain at least one relevant document.

Total number of pages of all documents relevant to the request (including exempt pages)

Number of agency documents falling within the terms of the request.

Number of pages of relevant documents to be exempted in full.

Number of pages of relevant documents to be released in part.

Number of documents for which access is by supervised inspection of the document.

Agencies may not charge for FOI requests to the extent that they relate to personal information about the FOI applicant

Applies to non-Commonwealth consultees (e.g. individuals, businesses, other governments). Only count each party once if referred to in multiple documents.

This amount takes into account any reductions to the cost as a result of the application involving personal information

The percentage discount to be applied if agency takes into account financial hardship or public interest under s 29 of the FOI Act.