Australian Government

Centrelink
giving you options

DECLARATION OF CONFIDENTIALITY

PRIVACY, SECURITY, FRAUD AWARENESS AND CONDUCT RESPONSIBILITIES

Australian Government | Centrelink
giving you options

Privacy, Security, Fraud Awareness and Conduct in Centrelink

All Employees

Centrelink is one of Australia's largest government employers and administers around 30% of all Australian Government outlays every year. It is an important role. Centrelink is privileged to make a real difference in the lives of many Australians.

Centrelink's success as an organisation is founded on our integrity as a business. We must maintain a high level of government and community confidence to successfully administer these programs and provide this support into the future.

To build and maintain this confidence in Centrelink, it is important that all employees and contractors have a strong understanding of their workplace responsibilities in relation to privacy, confidentiality, security, conduct and fraud awareness.

As a government agency, we have a clear responsibility to conduct all of our business to the highest ethical and professional standards. All government employees are expected to uphold the Australian Public Service (APS) Values and comply with the APS Code of Conduct as defined in the *Public Service Act 1999.*

In your job you are likely to handle personal information relating to Centrelink customers and/or employees. This information is provided for the purpose of performing your duties. As a Centrelink employee or contractor, you have an obligation to protect this information and handle it in accordance with specific legal requirements and standards.

Details are provided in this booklet. Your Team Leader and Privacy Officer will take you through this information to help you to understand and follow the rules relating to privacy and confidentiality while doing your job, and show you how to access more information.

It is important that you read this booklet and familiarise yourself with Centrelink's privacy and confidentiality legislation and security policies, as well as your personal responsibilities in relation to conduct and fraud awareness as a Centrelink employee.

Page 23 contains a DECLARATION OF CONFIDENTIALITY. New employees and contractors must sign the declaration before being given access to confidential information held by Centrelink. In this declaration you acknowledge that you agree to abide by the confidentiality rules detailed in this booklet.

JEFF WHALAN

Chief Executive Officer

PART A

Contents

CONTENTS

NOTE FOR TEAM LEADERS AND OFFICE TRAINERS:

You need to take new employees through parts A, B & C of this booklet before the Checklist and Declaration of Confidentiality are signed and forwarded to the appropriate Privacy Officer and HR Team.

In this booklet 'employee' refers to ongoing, non-ongoing and contracted employees.

PART A

Privacy and Confidentiality

Centrelink has a strong privacy culture that supports the rights of our customers and employees to have their personal information protected in accordance with Commonwealth law. Good privacy practices build confidence in Centrelink's ability to effectively deliver services on behalf of government. This booklet outlines some areas of concern that you should be aware of before gaining access to personal/protected information.

The foundation of Centrelink's privacy culture is our legal obligation to comply with the *Privacy Act 1988* and the confidentiality provisions contained in the various legislation we administer, for example, the *Social Security (Administration) Act 1999, A New Tax System (Family Assistance) (Administration) Act 1999* and *Student Assistance Act 1973.*

The confidentiality provisions contained within the legislation govern access to, use and disclosure of protected information in electronic or paper records of Centrelink or its policy departments. The confidentiality provisions in various legislation allow a person to obtain **protected information** only for the purpose of performing their duties.

The *Privacy Act 1988* contains the Information Privacy Principles (IPPs) that set the standards for the collection, storage, access, use and disclosure of **personal information**. The IPPs apply to Commonwealth departments and agencies. Protecting privacy is more than guaranteeing confidentiality. Centrelink must ensure that individuals are informed about what is happening to their information, and are able to participate in decisions about what is collected, who collects it and why.

As Centrelink continues to take on new business and administers a variety of legislation, it is **your responsibility** to ensure that you are fully conversant with your obligation to handle personal/protected information as allowed by the legislation.

While the confidentiality provisions in various acts administered by Centrelink apply to personal information collected under social security or family assistance law and other legislation administered by Centrelink, the *Privacy Act 1988* applies to the personal information of our customers, employees and other individuals whose information is held in Centrelink records.

What is a breach of confidentiality?

A breach of confidentiality occurs when someone looks at, makes a record of, uses or discloses protected information when it is not for the purpose of performing their duties under the relevant legislation.

There are severe penalties for employees who breach the confidentiality provisions. These include penalties under various legislation (including the *Crimes Act 1914*) of up to two years imprisonment. Ongoing and non-ongoing employees may also face sanctions under the *Public Service Act 1999* which may attract disciplinary measures such as fines, demotions or dismissal. Contracted employees may have contracts terminated.

PART A

What is a breach of Privacy?

A breach of privacy occurs where an act or practice of an agency breaches one of the Information Privacy Principles (IPPs) in the *Privacy Act 1988* or the Tax File Number (TFN) Guidelines issued by the Privacy Commissioner. Agencies are responsible for ensuring practices and procedures comply with the IPPs.

Under the *Privacy Act 1988* there are no penalties for the individual who breaches privacy; however, an employee may be subject to disciplinary action under the *Public Service Act 1999*, which may attract disciplinary measures such as fines, demotions or dismissal. Contracted employees may have their contracts terminated.

Browsing and Conflict of Interest

Access to personal information is on a 'need to know' basis in order for you to perform your duties. It is not provided for your private use. You do not have to disclose the information to someone else, just looking at a customer or employee record when you are not authorised for the purpose of carrying out your duties with Centrelink, is an offence under various legislation Centrelink administers. This is commonly known as **browsing.**

You are not authorised to access and/or process your own customer record or those of family, friends or other people where there may be, or may be perceived to be, a **conflict of interest.** This also includes people with whom you may have had or are having a dispute. You can, however, access your own personnel record on Infolink HR. If you are also a customer, you can register to use the **customer** online services channel **on the Centrelink website.** This allows you the same access to your record as other customers have. However, you must not access your own record using the Customer Account facility that is available to employees.

While it is acceptable for you to receive a request from a friend, relative or acquaintance for information or advice about the person's dealings with Centrelink, you should not be involved in processing the matter. This includes accessing the customer's or Centrelink employee's record. **A customer (including a colleague who is a customer) cannot authorise you to access their record** when such access would be contrary to Centrelink policy. For example, your mother cannot authorise you to look at her record, because Centrelink instructions clearly state that you cannot access or assess the records of family members. This type of access would be considered to be a conflict of interest.

If you are concerned about a possible conflict of interest you should speak to your Team Leader **before** dealing with that person or accessing their record. The Team Leader can authorise you to deal with the matter or reassign the case to another employee. The vast majority of privacy complaints come from people who know the Centrelink employee concerned, so this policy is in place to protect you against false allegations.

Some examples of unauthorised access, use and disclosure **include:**

- accessing a customer's, Centrelink employee's or contractor's record to get their address and home telephone number for personal reasons
- out of curiosity, looking up the records of people reported in the media
- accessing or processing a friend's or work colleague's claim for a payment or service from Centrelink
- accessing a neighbour's record because they cannot get through to the Call Centre

- accessing your own customer record because you are not confident that your claim has been assessed correctly
- accessing the record of a friend to let them know how much is owing on their Centrelink debt or when their form is due to be lodged
- creating, accessing or assessing a record with the intent to gain financially or otherwise
- looking up Infolink HR to get a work mate's home telephone number to invite them to lunch.

You must not disclose protected/personal information about customers or employees to third parties who are not authorised to receive this information.

All accesses to the records of customers and employees from the Income Security Integrated System (ISIS), Infolink FI and Infolink HR, are logged and monitored. Logging reports can be produced which show the exact date, time and screens accessed by employees. This is for the protection of both customers and Centrelink employees.

PRIVACY COMPLIANCE STRATEGY (PCS)

The Privacy Compliance Strategy (PCS) has been implemented to support Centrelink's commitment to its legislative obligations to protect the privacy and confidentiality of customer and employee information. The object of the PCS is to support a control framework of prevention, detection and deterrence of browsing and inappropriate access to customer and employee information.

The PCS reinforces Centrelink's ongoing determination to ensure that authorised employees only access customer and employee information **that is relevant to the direct performance of their duties.** To achieve this objective, proactive monitoring of accesses made by employees to the personal/protected information contained in Centrelink's records is carried out. Where access to a record appears to be unauthorised it will be referred for further investigation.

Reporting Privacy Incidents

All allegations regarding breaches of privacy and/or confidentiality should be reported to the Area Privacy Officer or the Privacy and Information Access Section in Legal Services Branch.

Individuals who believe their privacy has been breached can contact the Area Privacy Officer and may also lodge a complaint with the Federal Privacy Commissioner.

PRIVACY RESOURCES

More detail on how confidentiality and privacy legislation relates to you and your role with Centrelink is explained in the Privacy and Confidentiality Manual found in the Privacy Awareness Kit. This can be accessed online at **http://centrenet/corp/priv/index.htm**

- Privacy training videos:
  - *CLIPS (Centrelink Leading in Privacy Strategies)*
  - *Privacy Stakes*
- Privacy fact sheets/brochures:
  - *Starting with Privacy (for employees of Centrelink)*

PART A

  - *Your Right to Privacy* (for customers of Centrelink)
  - *Customer Research and You* (for customers of Centrelink)

- Privacy Training Modules
  - Basic Module
  - Call Centre Module
  - Freedom of Information (FOI) Module
  - Managers and Employees Dealing With Personnel Matters Module
  - Indigenous Customer Service Officers (ICSO) Module

Your Area Privacy Officer can help with your **privacy/confidentiality** enquiries and show you how to access the confidentiality legislation contained within various Acts administered by Centrelink. Contact details can be found on the Privacy and Information Access Section home page at: **http://centrenet/homepage/nso/servimp/privacy/index.htm** or email **PRIVFOI.NA.**

National Support Office (NSO) employees should contact the Privacy and Information Access Section in Legal Services Branch regarding training and advice.

PART B

Security Responsibilities

Centrelink is required to satisfy minimum standards for security set by the Government and contained in the *Commonwealth Protective Security Manual* (PSM). All staff have responsibility for meeting these security standards and may be held accountable for any failures or breaches of security. Breaches of security may result in action being taken under the Australian Public Service (APS) "Code of Conduct" provisions contained in section 13 of the *Public Service Act 1999.*

Centrelink's *Security Policy Manual* is a comprehensive document that will assist you to understand and apply the policies in your role as an employee of Centrelink. The Manual contains information about protective security, information security, personnel security and IT security. To help you to understand and comply with a number of relevant security policies, we have listed and summarised some of the security policies below.

1. Security Awareness

Employees shall take all reasonable steps to become familiar with and comply with the policies detailed in the Centrelink *Security Policy Manual* and the Commonwealth *Protective Security Manual.*

2. Security Identification and Authentication

Employees shall always wear identification. This is presently a current **Accesslink** card and a Centrelink name badge. Both must be worn at all times and be easily visible. Accesslink is the Smartcard system that allows employees to access Centrelink computer systems. Accesslink may also be used to provide building access.

Your Accesslink card is **your responsibility.** As the assigned cardholder, all access recorded against your Accesslink card will be deemed performed by you. You must protect your Accesslink card as well as your Personal Identification Number (PIN). Never record your PIN anywhere, at any time. Under no circumstance is your Accesslink card to be used by another person. All forms of authentication (e.g. Accesslink Cards, PINs, passwords, encryption codes etc.) used within Centrelink, are regarded as sensitive and are to be actively protected from disclosure and compromise.

Your Accesslink card will be valid for a maximum period of two years, at which time the photo identification and the validation date must be updated. It is the property of Centrelink and must be returned to your Team Leader/Manager or to your Accesslink officer when your employment with Centrelink ends.

3. Security Verification

Employees shall always check the credentials of persons on Centrelink premises. All visitors are required to sign a visitors' register and wear appropriate Centrelink identification.

4. Security Protection

Employees shall always ensure the protection of Centrelink's official information, assets, equipment, resources, employees and customers by adhering to Centrelink's security policy and procedures.

PART B

5. Information Protection

Centrelink collects, receives and develops information to fulfil its functions, and expects all employees who access or hold this information to protect it. This information is known as **"official information"** and must be handled with due care in accordance with authorised procedures.

Official information must be made available only to persons who have a legitimate need to know to fulfil their official duties or contractual responsibilities. The availability of official information should be limited to those who need to use or access the information to do their work. Therefore, if you don't need the information to do your work, you should not view or access such information. The need-to-know principle must be applied to all official information, except for public domain information.

6. Clear Desk Security Policy

Employees must ensure that all official information classified 'confidential' (including customer files and documents) and other valuable resources are secured appropriately when absent from the workplace. This includes being away from the workplace for short meetings and lunch.

Employees working in public contact areas or public access areas must ensure that all official information classified 'confidential' (including customer files and documents) and other valuable resources are secured appropriately when absent from their workstation. This includes any absence from the workstation for short or long periods.

Employees must not leave information which has a security classification of 'protected' level or higher unattended at any time. Any such information must be properly secured whenever absent from working areas during the day and before leaving at the end of the day.

Computer screenlock is part of the clear desk policy. Screenlock should be activated whenever you leave your workstation. To activate Screenlock, press the keys CTRL+ALT+DEL at the same time, and then press ENTER, or double click on the screen saver activation icon located at the bottom right of your computer screen.

Employees are to take all reasonable steps to control access to their workstation and shall not knowingly allow another person to use a workstation to which they are logged on and shall not leave a workstation unsecured or unattended after logging on.

7. Personnel Security Clearances

Occupants of certain positions may be required to undergo a security clearance before they can obtain access to **security classified** information or resources. Your Team Leader or Business Line Manager should advise you whether a security clearance is needed to perform your work. Further advice may be obtained from the Agency Security Adviser (ASA) or the Personnel Security Officer.

8. IT Security

Employees shall conform to all security measures and procedures in place, to ensure that sensitive I&T equipment or valuable assets are protected from theft, damage and unauthorised access. Refer 6 above.

PART B

9. Use and Provision of Computing Facilities

Electronic, computing and general facilities are provided for legitimate Centrelink business. Electronic and computing facilities may be used for 'limited personal use' provided that such use does not:

- interfere with an employee's duties and obligations to Centrelink
- require access outside normal working hours, and/or
- include usage deemed inappropriate or unacceptable by Centrelink and the Government. Refer to Centrelink's *Use of Centrelink's Electronic Facilities* handbook, which is available from the People Handbook, under the topic 'Working' or at:

http://centrenet/homepage/divpeople/brwrep/handbook/working/wkg055.htm

Centrelink will, at its discretion, monitor and log the use of its systems (including e-mail, Internet and mainframe) to ensure that the integrity and confidentiality of its information is maintained.

10. Intellectual Property and Copyright

Employees are to maintain the confidentiality, integrity and copyright of all assets developed, used and purchased by Centrelink. In particular, employees:

- shall only use software in accordance with the approved licence agreements
- shall not, without appropriate authority, make copies of Centrelink owned or leased IT assets for any purpose
- shall report all instances of IT assets misuse to their Team Leader/Manager and the IT Security Adviser (ITSA).

11. Reporting of Security Incidents

Employees have a duty to report all security violations, breaches and incidents to their Team Leader and/or Manager and the Agency Security Adviser (ASA) as soon as possible so that prompt remedial action may be taken. To report a security incident, you must ensure that a Security Incident Report form is completed. These forms can be accessed from the Security homepage on CentreNet.

SECURITY VIOLATIONS/BREACHES

Where there is evidence of a breach of security policies, standards and/or procedures, a preliminary investigation will be undertaken and/or specific or directed auditing activities will be authorised. The outcomes of such actions may result in:

- the matter being referred for action in accordance with the procedures for determining whether an employee has breached the APS Code of Conduct (see the People Handbook)
- confirmation that a breach of a contractual agreement has occurred, thus initiating an internal investigation
- confirmation that a criminal act has occurred, thus initiating a criminal investigation in conjunction with police authorities and in accordance with the Criminal Code Act
- relevant security awareness programs being reinforced, (eg training, retraining)
- security policies, standards or procedures being modified.

PART B

Where an allegation is proven against an employee, sanctions may result in:

- reprimand
- a deduction from salary, by way of a fine that does not exceed two percent of the employee's annual salary
- reduction in salary
- reassignment of duties
- reduction in classification
- termination of employment.

SECURITY RESOURCES

More information about security is available online at: **http://centrenet/homepage/divitcore/britsip/itspa/itspa.htm** or by sending an email to SECURITY.POLICY

From this intranet site you can also access the *Security Policy Manual*, information about the **Agency Security Adviser (ASA)**, the **Agency IT Security Adviser (ITSA)** and other security contact information.

The ASA and Security Contact Officers can advise you on protective security matters and security training and the ITSA can advise you on IT security matters.

PART C

Fraud Awareness and Conduct Responsibilities

Centrelink is committed to the prevention, detection and deterrence of internal fraud and misconduct. You need to ensure that you understand your responsibilities in controlling fraud and adhering to the APS Values and APS Code of Conduct during your employment with Centrelink.

DEFINITION OF FRAUD

Centrelink has separated fraud into the following three areas to define the type of fraud that affects Centrelink.

1. **Administrative Fraud**—occurs when Centrelink employees use resources for purposes other than those for which they were provided. This can involve stealing property for personal use, manipulating salaries or incorrectly claiming overtime. It may also involve people outside Centrelink attempting to fraudulently obtain Centrelink's administrative funds.
2. **Information Fraud**—is the theft or misuse of information held by Centrelink. It occurs when employees make inappropriate use of information they have access to as part of their duties. It can include the sale or provision of customer details to a third party (e.g. a private investigator), or browsing customer records for personal interest.
3. **Payment Fraud**—can involve customers, non-customers and/or Centrelink employees (internal fraud). It involves people lodging false claims to receive payments that they are not entitled to. It also occurs when Centrelink employees misappropriate funds by making payments to people for personal gain or to a third party who would otherwise be ineligible.

The *Commonwealth Fraud Guidelines* define fraud against the Commonwealth as **"Dishonestly obtaining a benefit by deception or other means".**

This definition includes:

- theft
- obtaining property, a financial advantage or other benefit by deception
- causing loss, or avoiding or creating liability by deception
- providing false or misleading information to the Commonwealth, or failing to provide information where there is an obligation to do so
- making, using or processing forged or falsified documents
- bribery, corruption, or abuse of office
- unlawful use of Commonwealth computers, vehicles, telephones and other property or services
- relevant bankruptcy offences
- any offence of a like nature to those listed above.

PART C

All Centrelink employees must:

1. adhere to all requirements specified within legislation, policy and direction
2. observe directions from the Chief Executive Officer, General Manager—Audit and Risk, and Business Manager—Internal Fraud and Ethics Section, in the conduct of enquiries related to suspected fraud and misconduct
3. report any suspected incidents of fraud and misconduct
4. ensure that the APS Values and APS Code of Conduct are observed at all times.

The objective of this direction is to ensure that:

- all Centrelink managers and business teams are aware of their responsibilities in the management of suspected fraud and misconduct
- all employees are aware of their individual obligations to comply with policy, guidelines and direction
- every employee adopts Centrelink's fraud prevention measures and reports any suspected incidence of employee fraud and misconduct.

It is the duty of all employees to adopt fraud and misconduct prevention measures and to report any suspected incidents.

ETHICS

Section 10 of the *Public Service Act 1999* deals with the personal behaviour of Australian Public Service (APS) employees. Section 10(1)(d) of this Act requires that APS employees behave with the highest ethical standards. Ethics are not simply about acting to the law or in compliance with policy, they are also about acting with consideration to values, perspective, judgement and consequences.

At work this means:

- supporting ethical work practices through your own behaviour or decision-making
- encouraging these principles in others
- understanding Centrelink's position on ethical issues
- considering the effect of individual behaviour and consequences of action upon others and the organisation as a whole
- being honest, truthful and forthright with colleagues, management and external customers in a manner that is sensitive to their concerns, that does not mislead them and that does not disclose confidential information
- maintaining a high level of integrity in the face of ethical dilemmas or unethical standards in others by standing up for what is right
- resisting pressure to do the wrong thing or to compromise these standards for short term gain
- taking personal responsibility.

As Centrelink employees, we are in a position of trust with regard to using Centrelink's equipment and resources, protecting Centrelink's assets, maintaining security controls and procedures and effectively reporting and documenting our activities.

PART C

Centrelink expects all employees to approach their responsibilities, work and dealings with colleagues and customers in accordance with the APS Values and comply with the APS Code of Conduct.

Reporting Internal Fraud and Unethical Behaviour

Centrelink employees are required to report all suspected cases of internal fraud and misuse to either their Office Manager/Business Manager, Area/National Manager or the Internal Fraud and Ethics Section, Centrelink Audit Risk and Ethics Division.

Investigations and Penalties

Possible courses of action depending on the result of an investigation:

- code of conduct processes leading to sanctions under the *Public Service Act*, and/or
- criminal processes taken over by the Australian Federal Police (AFP) and/or the Director of Public Prosecutions (DPP).

Non-compliance with legislation and Centrelink policy may result in a code of conduct investigation being carried out and penalties under Section 15 of the *Public Service Act 1999* being imposed. Where a criminal offence has been committed, penalties would be imposed under the Criminal Code Act 1995.

RESOURCES

To query or confirm any of Centrelink's administrative policies, to report cases of administrative loss, theft, misuse and damage, contact the Internal Fraud & Ethics section. Contact details can be found on their home page at: **http://centrenet/homepage/divaudit/cars/index.htm** or email: ADMINISTRATIVE FRAUD

REFERENCES

- *Financial Management and Accountability Act 1997*
- Financial Management and Accountability Act Regulations
- *Public Service Act 1999*
  - Part 3, Section 10: Australian Public Service Values
  - Part 3, Section 13: Australian Public Service Code of Conduct
- *The Criminal Code Act 1995*
- Chief Executive Instructions
- *Privacy Act 1988*
- Commonwealth Fraud Control Guidelines
- Fraud Control Plan
- Fraud Control Action Plans
- People Handbook
- Procurement and Contracting Manual

PART D

Legislation and Definitions

Social Security (Administration) Act 1999 (SSAA)

A New Tax System (Family Assistance) (Administration) Act 1999 (FAAA)

Student Assistance Act 1973 (SAA)

SSAA	FAAA	SAA	CONTENT
201-202	161-162	351	Protection of personal information–who can access protected information, how it can be used and to whom it may be disclosed
203	163	352	Offence–unauthorised access.
204	164	353	Offence–unauthorised use and disclosure.
205	165	357-358	Offence–soliciting disclosure of protected information.
206	166	359	Offence–offering to supply protected information.
207	167	354	Protection extends to courts, tribunals, proceedings etc.
208-209	168-169	355-356	Secretary's certificates in relation to disclosure of information and guidelines for exercise of Secretary's power.
210	170	360	Officer's oath or declaration.
		361	Freedom of Information Act not affected.

PART D

Definition of Officer

s201 of the *Social Security (Administration) Act 1999* defines an 'officer' as:

(a) a person who is or has been an officer within the meaning of subsection 23(1) of the 1991 Act; or

(b) a person who is or has been appointed or employed by the Commonwealth and who, as a result of that appointment or employment, may acquire or has acquired information concerning a person under the social security law or the *Farm Household Support Act 1992*; or

(c) a person who, although not appointed or employed by the Commonwealth, performs or did perform services for the Commonwealth and who, as a result of performing those services, may acquire or has acquired information concerning a person under the social security law or the *Farm Household Support Act 1992*.

Protected Information

The *Social Security Act 1991* defines 'protected information' as:

(a) information about a person that is or was held in the records of the Department or of the Agency; or

(b) information about a person obtained by an officer under the family assistance law that is or was held in the records of the Australian Taxation Office or Medicare Australia; or

(c) information to the effect that there is no information about a person held in the records of one or more of the following:

(i) the Department;

(ii) the Agency;

(iii) the Australian Taxation Office;

(iv) Medicare Australia.

The *A New Tax System (Family Assistance) (Administration) Act 1999* defines 'protected information' as:

(a) information about a person that is or was held in the records of the Department or the Commonwealth Service Delivery Agency; or

(b) information about a person obtained by an officer under the family assistance law that is or was held in the records of the Australian Taxation Office or Medicare Australia; or

(c) information to the effect that there is no information about a person held in the records of an agency.

PART D

Personal Information

The Privacy Act 1988 states:

'Personal information' means information or an opinion (including information forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

Official Information

As defined in the *Commonwealth Protective Security Manual (2000)*: is any information developed, received or collected by or on behalf of Government, through its agencies and contracted providers.

Security Classified Information

As defined in the *Commonwealth Protective Security Information Manual (2000)*: is official information that, if compromised, could threaten the security or interests of individuals, groups, commercial entities, government business and interests, or the safety of the community. Examples of this type of information include information on law enforcement operations and personal information concerning members of the public. Examples of classified information include:

- STAFF-IN-CONFIDENCE
- SECURITY-IN-CONFIDENCE
- CUSTOMER-IN-CONFIDENCE
- CABINET-IN-CONFIDENCE
- BUDGET-IN-CONFIDENCE
- PROTECTED

PART D

Guide to the Information Privacy Principles (IPPs) as contained in the *Privacy Act 1988*

IPP 1 COLLECTION

Agencies can only collect personal information:

- for a lawful purpose that is directly related to their functions, and necessary for or directly related to that purpose; and
- Centrelink must not collect personal information in a way that is unlawful or unfair.

IPP 2 COLLECTION

When an agency asks for personal information directly from the person who that information is about, we must take whatever steps are reasonable to make sure the person is aware of the following details:

- why the agency is collecting the information
- the agency's legal authority (if any) to collect the information
- to whom the agency usually gives that kind of information.

IPP 3 COLLECTION

When an agency asks for personal information, we must take reasonable steps to make sure that:

- the information the agency collects is relevant, up to date and complete
- the agency does not collect information in an unreasonably intrusive way.

IPP 4 STORAGE AND SECURITY

The agency must ensure that personal information is stored and kept secure against:

- loss
- unauthorised access, modification, disclosure
- other misuse.

IPPS 5, 6 AND 7 ACCESS

Covers:

- information relating to records kept by the record keeper
- access to records containing personal information
- alteration of records containing personal information.

USE IPP 8

Agencies must take reasonable steps to ensure that the personal information it uses is accurate, up to date and complete.

USE IPP 9

An agency must only use personal information for a purpose to which the information is relevant.

PART D

USE IPP 10

Limits are set on how an agency may use personal information.

General rule: An agency may only use personal information for the particular purpose for which it obtains the personal information.

Exceptions: There are situations in which an agency may use personal information for purposes other than that for which it obtains the personal information.

These are:

- the individual consents to the use;
- the use is necessary to protect against a serious and imminent threat to a person's life or health;
- the use is required or authorised by or under law;
- the use is reasonably necessary to enforce the criminal law or law imposing a pecuniary penalty, or to protect the public revenue; **or**
- the use is directly related to the purpose for which the agency obtained the information.

IPP 11 DISCLOSURE

An agency may only disclose personal information to the person the information is about, and not to any other person or organisation unless one or more of the situations below apply:

- the individual consents to the disclosure;
- the disclosure is necessary to protect against a serious and imminent threat to a person's life or health;
- the disclosure is required or authorised by or under law;
- the disclosure is reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty, or to protect the public revenue; **or**
- the person the information is about has been told in a valid IPP 2 notice, or is otherwise likely to know, that kind of disclosure is commonly made.

PART D

APS Code of Conduct

(1) An APS employee must behave honestly and with integrity in the course of APS employment.

(2) An APS employee must act with care and diligence in the course of APS employment.

(3) An APS employee, when acting in the course of APS employment, must treat everyone with respect and courtesy, and without harassment.

(4) An APS employee, when acting in the course of APS employment, must comply with all applicable Australian laws. For this purpose, Australian law means:

a. any Act (including this Act), or any instrument made under an Act; or

b. any law of a State or Territory, including any instrument made under such a law.

(5) An APS employee must comply with any lawful and reasonable direction given by someone in the employee's agency who has authority to give the direction.

(6) An APS employee must maintain appropriate confidentiality about dealings that the employee has with any Minister or Minister's member of staff.

(7) An APS employee must disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with APS employment.

(8) An APS employee must use Commonwealth resources in a proper manner.

(9) An APS employee must not provide false or misleading information in response to a request for information that is made for official purposes in connection with the employee's APS employment.

(10) An APS employee must not make improper use of:

a. inside information; or

b. the employee's duties, status, power or authority, in order to gain, or seek to gain, a benefit or advantage for the employee or for any other person.

(11) An APS employee must at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.

(12) An APS employee on duty overseas must at all times behave in a way that upholds the good reputation of Australia.

(13) An APS employee must comply with any other conduct requirement that is prescribed by the regulations.

PART D

	THE CRIMES ACT 1914
Section 70	This section says a Commonwealth officer must not publish or communicate any confidential or sensitive document or fact they are aware of in their capacity as a Commonwealth officer, unless it is to an authorised person. This also applies to a person who previously held a position as a Commonwealth officer.
	THE CRIMINAL CODE ACT 1995
	This Act contains general prohibitive principles that apply to all Commonwealth employees. The following restrictions are not exclusive and are only offered as a guide. For more information consult the *Criminal Code Act 1995*. In summary, this Act: • prohibits Commonwealth employees from destroying, stealing or intending to steal property belonging to the Commonwealth • has penalties against Commonwealth employees behaving in a dishonest manner to commit or conspire to commit fraud • forbids a Commonwealth employee asking for, receiving or obtaining a benefit for himself, herself or another person • prohibits a person from intentionally and with authority obtaining access to data stored in a Commonwealth computer. (This is a 'browsing' offence under the *Criminal Code Act 1995*.) • prohibits a person damaging (destroying, erasing or altering) data held in a Commonwealth computer • prohibits a Commonwealth employee dishonestly using information gained in their capacity as a Commonwealth employee. Penalties for breaches under this Act can range up to 10 years imprisonment.
	GOVERNMENT PROCEDURAL STANDARDS FOR SECURITY
	Some procedural standards are: • Commonwealth Protective Security Manual • Australian Communications Electronic Security Instructions (ACSI) 33 • Gateway Certification Guide • Cabinet Handbook

PART E

Checklist

Inductee's name:

Start date: / / Office:

Inductor's name/position

- ☐ Issued with brochure *Starting with Privacy.*
- ☐ Read and understood the *Use of Centrelink's Electronic Facilities* topic in the People Handbook.

Received an explanation of privacy, confidentiality, security, fraud and conduct responsibilities, including:

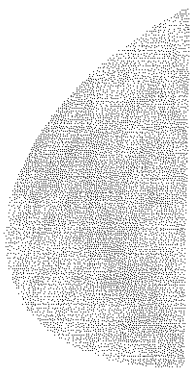
- ☐ the confidentiality provisions
- ☐ what happens if you breach confidentiality
- ☐ conflict of interest
- ☐ browsing
- ☐ what the Information Privacy Principles (IPPs) mean for Centrelink
- ☐ handling personal information
- ☐ document disposal
- ☐ explanation of the Declaration of Confidentiality and signature
- ☐ explanation of the use of Centrelink's Electronic Facilities
- ☐ an overview of the APS Code of Conduct Principles
- ☐ definition of official information
- ☐ definition of security classified information
- ☐ security of Accesslink cards, PINs, passwords etc
- ☐ how to secure your workstation (screenlock)
- ☐ clear desk policy
- ☐ 'need to know' principle
- ☐ process for reporting security violations, breaches and problems
- ☐ what happens when there is a breach of security policies, standards or procedures
- ☐ introduction to Centrelink Reference Suite—reference material for security, privacy, conduct and fraud awareness
- ☐ Fraud Control Plan 2004—2006
- ☐ location of additional resources
- ☐ team specific material
- ☐ name forwarded to Area Privacy Officer for security and privacy awareness training.

Inductee's signature / /

Inductor's signature / /

Please forward copies of this form to the Area Privacy Officer (for security and privacy awareness training), and HR (for filing purposes, along with the signed Declaration of Confidentiality).

Tear off



PART F

Declaration of Confidentiality

All employees are required by the Chief Executive Officer of Centrelink to make a Declaration of Confidentiality.

Tear off

DECLARATION

I, ...

of .....

(office)

AGS Number (where applicable) .....

hereby declare that I have been provided with the 'Declaration of Confidentiality, Privacy, Security, Fraud Awareness and Conduct Responsibilities' booklet.

I understand that this booklet details some of my privacy and confidentiality obligations and that these obligations arise under legislation.

I have read and understood Parts A (Privacy and Confidentiality), B (Security Responsibilities) and C (Fraud Awareness and Conduct Responsibilities) of this booklet and undertake to read Part D (Legislation and Definitions).

I agree to abide by the rules set out in this booklet

	/ /

Witness to complete:

Declared at .....

(office)

This..... day of..... 20

Before me .....

(Witness Name)

.....

(Witness Signature)