6

19

FINAL REPORT OF THE DECISION MAKER ON SUSPECTED BREACH OF THE CODE OF CONDUCT BY S 22 / 47F

1. As selected in accordance with paragraph 2 of the Procedures for Determining Breaches of the Code of Conduct (the Code of Conduct Procedures), by Mark le Dieu, National Manager, People Services Branch, and as referred to me by S 22/47F, National Manager, S 47F, I am required to:

   a. investigate an allegation that you may have breached the Australian Public Service Code of Conduct;

   b. determine whether you did breach the Code of Conduct; and

   c. in the event that I find you did breach the Code of Conduct, make a recommendation on what, if any, sanction(s) should be imposed.

SUSPECTED BREACH OF THE CODE OF CONDUCT

2. It is suspected that you may have failed to comply with laws relating to unauthorised access to Centrelink information and failed to comply with Centrelink's 'unauthorised access' policies by accessing protected information held in Centrelink's Income Support Information System (ISIS) and On-Line Search (OLS) records without a legitimate business reason for doing so. Specifically, it is suspected that you may have made unauthorised access on thirteen (13) separate occasions to the protected information of:

   - yourself, on one (1) occasion on 9 December 2008;
   - your sister in law S 22/47F ll, on one (1) occasion on 27 May 2009;
   - your brothe S 22/47F l, on one (1) occasion on 27 May 2009;
   - your siste S 22/47F ll, on four (4) separate occasions from 27 May 2009 to 26 October 2009;
   - your brothe S 22/47F ll, on one (1) occasion on 9 June 2009;
   - your sister in law S 22/47F l, on one (1) occasion on 9 June 2009;
   - your siste S 22/47F n, on three (3) separate occasions from 27 May 2009 to 3 September 2009; and,
   - your brother in law S 22/47F n, on one (1) occasion on 3 September 2009.

3. My task is to establish whether your suspected conduct occurred and if so, whether it was a breach of the Code of Conduct.

4. I suspect that your conduct may be in breach of the following elements of the 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;

   (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 the Public Service Act 1999), or any instrument made under an Act; or

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

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

(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.

LEGISLATION/POLICY/INSTRUCTIONS

5. In conducting this investigation I have had regard to the following legislation, policy and instructions:

   a. APS Values, section 10(1) of the *Public Service Act 1999* (the Act). The APS Values have applied since 5 December 1999 and underpin the behaviours expected of APS employees and their relationships with the government and parliament, the public, and each other.

   b. Code of Conduct, section 13 of the *Public Service Act 1999* (the 1999 Act). The Code of Conduct has applied since 5 December 1999 and sets out the standards of conduct required of APS employees.

   c. Centrelink Procedures for Determining Breaches of Code of Conduct, which were established under subsection 15(3) of the Public Service Act 1999 and must be complied with in determining whether an APS employee has breached the Code of Conduct.

   d. subsection 203(1) of the *Social Security (Administration) Act 1999*, which has applied since 20 March 2000 and has been amended from time to time. Effectively, this provision makes it an offence for a person to intentionally access protected information in Centrelink records if the person is not authorised to obtain that information and knows that the information is protected information.

   e. subsection 204(1) of the *Social Security (Administration) Act 1999*, which has applied since 20 March 2000 and has been amended from time to time. Effectively, this provision makes it an offence for an unauthorised person to intentionally use, record or disclose protected information in Centrelink records if the person knows that the information is protected information.

   f. Centrelink Privacy and Confidentiality Manual Chapter 3, titled 'Storage and Security of Personal/Protected Information', which has applied since January 2003 and has been amended from time to time. This Chapter of the Manual states that a person whose information is held by Centrelink has a right to expect that Centrelink will hold it securely, and will ensure that access to the information is permitted only for legitimate purposes.

   g. Centrelink 'Declaration of Confidentiality/Privacy, Security, Fraud Awareness and Conduct Responsibilities' booklet (previously known as the 'Declaration of Confidentiality/Security and Privacy Responsibilities' booklet or the 'Rules for the Handling of Personal/Protected Information' booklet), which is referred to in this report as the Confidentiality Booklet. The Confidentiality Booklet is provided to employees who undertake training in privacy or information security awareness. The Confidentiality Booklet contains a summary of the 'unauthorised access' rules

and a Declaration of Confidentiality, which is signed by each employee who receives the Confidentiality Booklet.

h. Chief Executive's Instruction 20, 'Unauthorised Access to Centrelink Customer Records and the Personnel Records of Centrelink Employees', which has applied since 2 December 2005 and has been amended from time to time. This Instruction provides direction to employees regarding access, use and/or disclosure of personal or protected information, and conflict of interest matters.

EVIDENCE AND OTHER MATERIAL

6. In the course of my investigation, I have considered the following evidence and material:

   a. Information from your Personal Employment File, such as your public service history and declaration of confidentiality;

   b. Information from your Infolink Personnel Record, such as personal details, date specifications, pay levels and organisational assignments etc;

   c. Privacy Incident Investigation Report from S 22/47F Senior Privacy Officer, Legal Services and Procurement Branch. Please note that any personal information contained in the Privacy Incident Investigation Report which is not relevant to the matter being investigated has been redacted;

   d. copy of a Declaration of Confidentiality form signed and dated by you on 13 August 2008;

   e. records of Declaration of Confidentiality forms, electronically acknowledged by you on 19 August 2008 and 12 August 2009; and

   f. your response to the draft report, which you sent to me via email on 9 March 2010.

CENTRELINK'S 'UNAUTHORISED ACCESS' RULES

7. I am satisfied that Centrelink has provided staff with clear guidance about accessing customer records in circumstances where there may be a conflict of interest. In particular, Centrelink has unequivocally instructed staff not to handle cases concerning ex-partners, family, relatives or friends and/or acquaintances, and not to access their own customer records.

8. I am also satisfied that, to the extent that they provide direction to employees, the Chief Executive's Instructions I have referred to in this report constitute lawful and reasonable directions given by someone in Centrelink (or its predecessor, the Department of Social Security) who had authority to give the direction.

9. Chief Executive's Instruction 20 relevantly states:

   20.01 When accessing personal information held in the records of Centrelink, all employees must comply with Centrelink's privacy and confidentiality policy regarding access, use and.or disclosure of personal or protected information set out in:

   (a) Centrelink Privacy Awareness Kit

   (b) The Declaration of Confidentiality booklet that contains the 'Rules for Handling Personal/Protected Information'

20.02 In all their dealings with customers and/or other staff, employees must ensure that they deal with conflicts of interest, real or apparent, in accordance with the policy set out in:

(a) Centrelink Privacy Awareness Kit

(b) Centrelink People Management Handbook

(c) Centrelink Ethics Resource Kit

10. Chapter 3 of the Privacy and Confidentiality Manual relevantly states:

3.061 Being a Centrelink employee does not automatically authorise an individual to access protected information. Employees are given access to Centrelink computer and paper records in order for them to carry out their prescribed duties. Access to protected information is not provided for private use therefore employees must not access computer or paper records of customers or employees out of personal interest or curiosity...

3.063 Some examples of browsing include accessing:

- your own customer record;
- the customer database or Infolink to:
  - obtain a friend's birth date and/or address to send a greeting card;
  - obtain a friend or relative's telephone number which may be unlisted in order to contact them on a social/personal basis etc;
- the records of people reported in the press;
- neighbours records out of curiosity;
- the records of friends and relatives to find out what their income or assets might be;
- a customer record on behalf of a friend or relative;
- a friend's records to see how their claim is progressing or to see if it has been assessed correctly;
- a work colleagues record at his or her request;
- using 'live' records for group training purposes; and
- a customer's record who is the subject of a tip-off if it is not part of the staff member's job to do so.

3.064 Public confidence in the integrity of the public service is vital to the proper operation of government. Where the community perceives a conflict of interest that confidence is jeopardised. A conflict of interest occurs when an employee's personal affairs, financial or other interests conflict with the performance of their official duties...

3.067 There would be as conflict of interest where the employee has a personal interest in the person whose record is being accessed. For this reason an employee must not access and/or process their own customer record or those of family, ex family, friends, close personal acquaintances, neighbours [or] work colleagues without authorisation from their team leader...

3.068 The restriction does not apply to everyone an employee knows as a casual acquaintance. The test is whether the acquaintance with the customer could be seen

by a third person to be to the customer's advantage in his or her dealings with Centrelink...

3.071 If circumstances make it unavoidable for an employee to access the record of a friend, relative or acquaintance, the problem of conflict of interest can be overcome by advising his or her team leader/manager of the need **before** accessing the record. With the team leader's permission, the record may then be accessed and/or assessed. A record of this authorisation will need to be kept, possibly in a DOC created by the team leader on the customer record [or] in a secure office register signed by the team leader...

3.072 **A customer cannot authorise an employee** to access their record when such an access would be contrary to Centrelink practice. For example, an employee's mother cannot authorise them to look at her record because Centrelink instructions clearly state that an employee must not access or assess the records of family members....

3.101 A Centrelink employee may inadvertently access the customer record of a family member, friend, close personal acquaintance, neighbour etc. If this happens the employee must immediately speak with their team leader or manager and explain the situation. The team leader or manager must make a note of the 'inadvertent' access in a secure office register...

11. The Confidentiality Booklet relevantly states:

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 personal use. You do not have to disclose the information to someone else, just looking at a customer or employee's record when you are not authorised 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.

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 including 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** where such access would be contrary to Centrelink practice. 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.

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.

12. I have reproduced the above quotes to establish the basis for my finding that Centrelink has provided guidance on these matters. In making my findings, I have relied on the whole of the above quoted Chief Executive's Instructions, along with the other legislation, policy and instructions referred to in this document.

13. I am satisfied that:

a. Centrelink had specifically prohibited you from accessing customer records and processing activities concerning you and your immediate family, and/or acquaintances; and

b. Centrelink had expressly indicated that a failure to follow these rules might result in disciplinary action.

ACTION REQUIRED BY YOU IN RESPONSE TO INADVERTENT ACCESS

14. The Confidentiality Booklet relevantly states:

> 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.

15. Centrelink's Privacy and Confidentiality Manual relevantly states:

> 3.071 If circumstances make it unavoidable for an employee to access the record of a friend, relative or close personal acquaintance, the problem of conflict of interest can be overcome by advising his or her team leader/line manager of the need before accessing the record. With the team leader/line manager's permission, the record may then be accessed and/or assessed. A record of this authorisation must be made by the team leader/line manager who has authorised the access. To do this the team leader/line manager must access the customer record themselves and record an 'AAA' enquiry type DOC on the customer's record containing the authorised employee's logon id details and the date of the access they are approving. The DOC automatically records the logon id of the authorising team leader/line manager when it is applied.
>
> 3.101 A Centrelink employee may inadvertently access the customer record of a family member, friend, close personal acquaintance, neighbour etc. If this happens, the employee must remove themselves from the situation, notify their team leader/line manager and explain the situation, then record the incident in the Inadvertent Access Register, accessed from the Privacy and Information Access section homepage....

16. Since July 2007, a national online register has been in operation enabling employees to directly report occasions of inadvertent access. Prior to this, employees were required to notify their team leader/manager who would appropriately record the report and the action taken.

17. The Privacy Officer, S22/47F, has indicated that there is no record of you having reported inadvertent accesses to any of these Centrelink customer records.

YOUR KNOWLEDGE OF CENTRELINK'S 'UNAUTHORISED ACCESS' RULES

18. I have considered what knowledge you had, or should have had, of Centrelink's rules concerning accessing customer records concerning you, your family and/or acquaintances, including other Centrelink employees.

19. Personnel records indicate on 11 August 2008, you were engaged as an ongoing employee of Centrelink. You are now a Customer Service Advisor at the APS 4.2 level, working in th Section 47F

20. In summary, you have worked at Centrelink for a period of over 18 months. I note that as at the date of the last suspected unauthorised access on 26 October 2009, you had worked at Centrelink for a period of over 14 months.

21. Since 1992, Centrelink (and its predecessor, the Department of Social Security) has displayed computer messages on access to the Customer database to remind employees of their responsibilities concerning access to records concerning immediate family members, friends and/or acquaintances. From November 1994, the Centrelink mainframe randomly generated 25 messages, five of which directly relate to Centrelink's 'unauthorised access' rules. The text of these messages is set out below.

    a. Protecting client information is your responsibility. Accessing client or staff information when it is not required as part of your job is an offence. Penalties include fines, imprisonment and disciplinary action. All access to computer records is logged.

    b. Protecting client information is your responsibility. You may be approached by friends, relatives or a close personal acquaintance who knows that you work for the department. They may ask you to amend FA/FAS entitlement records or the like. Staff may not access friends' files (even in the course of your duties). This can lead to a clash of interest. Friends and family should be told to approach the office through the proper channels. If files of any of the above are given to you as part of your workload tell your supervisor who will reassign them to another staff member.

    c. Avoiding Conflict of Interest is your responsibility. Staff may not access their personal departmental client files nor those of their family and friends. This can lead to a Conflict of Interest.

    d. The price of privacy is eternal vigilance.

    e. Confidentiality is your responsibility. You may only access records necessary in the performance of your duties. Browsing is a criminal offence. All computer access is logged. The department can now tell if you have accessed a record.

22. The above messages have been supplemented by the following messages, launched in October 1998.

    a. Browsing: you don't have to give out the information to someone else, just looking at customer or staff records when you are not authorised is an offence.

    b. Family & friends deserve privacy too! You are not authorised to access the records of family, friends & close associates.

23. The above messages have also been supplemented by the following message, launched in March 1999.

    a. Staff are not authorised to access or assess their own customer record.

24. All employees are obliged and reminded to lock their keyboard every time they leave their desk. In any case, an unattended computer keyboard will lock after 10 minutes. I am satisfied that during your employment with Centrelink the above-mentioned messages will have provided you with daily reminders of your obligation to comply with Centrelink's 'unauthorised access' policies.

25. On 19 August 2008 you attended a Centrelink Privacy/Disciplinary Awareness Session at S 47F The session addressed a range of issues about access to

customer records, including unauthorised browsing and conflicts of interest. The session also addressed the consequences of failing to comply with Centrelink's 'unauthorised access' rules.

26. On 13 August 2008 you signed a form to indicate that you had received the Confidentiality Booklet. You certified that you had read and understood Parts A (Privacy and Confidentiality), B (Security Responsibilities) and C (Fraud Awareness and Conduct Responsibilities) of the Confidentiality Booklet and undertook to read Part D (Legislation and Definitions). You also agreed to abide by the rules set out in the booklet. The Confidentiality Booklet clearly establishes that employees are not entitled to access their own records and the records concerning family and/or acquaintances.

27. Since January 2008, Centrelink officers have received an e-mail annually on their commencement anniversary advising them that there is a Declaration of Confidentiality to acknowledge in the Inbox of their Infolink Personnel record. Officers are required to log into Infolink, select the Electronic Declaration of Confidentiality action item and acknowledge that they have read, understood and agree to abide by the rules contained in the Declaration of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities booklet. The CEO has directed that all officers must electronically acknowledge their obligations annually on their commencement anniversary. Your Infolink Personnel record indicates that on 19 August 2008 and 12 August 2009, you electronically acknowledged Declarations of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities.

28. On the basis of this evidence, I am satisfied that you knew, or ought to have known, that:

    a. accessing records and processing activities concerning you, your family and/or acquaintances is not permitted by Centrelink;

    b. accessing records and processing activities concerning you, your family and/or acquaintances might constitute a conflict of interest; and

    c. such conduct might result in disciplinary action.

YOUR SUSPECTED CONDUCT

29. Attached to the draft report that was delivered to you, was a Privacy Incident Investigation Report. When provided to me, the Privacy Incident Investigation Report annexed CRAM Reports. The relevant details from the CRAM Reports were set out in the Privacy Incident Investigation Report. Accordingly the CRAM Reports were not included in my draft report. Arrangements were however made for you to view these, had you wished to do so.

30. The Privacy Incident Investigation Report describes and analyses evidence which tends to suggest that you have accessed your own Centrelink customer record and those of seven (7) of your family members. Specifically, I note that it appears you have made unauthorised access to the Centrelink customer records concerning:

- yourself; on one (1) occasion on 9 December 2008;
- your sister in law, S 22/47F ; on one (1) occasion on 27 May 2009;
- your brothe S 22/47F on one (1) occasion on 27 May 2009;
- your sister, on four (4) separate occasions from 27 May 2009 to 26 October 2009;

- your brother, [redacted] on one (1) occasion on 9 June 2009;
- your sister in law [redacted] on one (1) occasion on 9 June 2009;
- your siste[redacted]n; on three (3) separate occasions from 27 May 2009 to 3 September 2009; and,
- your brother in law [redacted] on one (1) occasion on 3 September 2009.

31. I have adopted the content of the Privacy Incident Investigation Report as my findings of fact in relation to your access to your own Centrelink customer record and those of seven (7) of your family members.

32. On 1 December 2009, you provided a statement to the Privacy Officer in response to these allegations. In your statement, you acknowledged that you had accessed these records with authorisation, stating that *'there is no reason for what I have done, it was completely wrong of me to have accessed these records'.*

33. Whilst you indicated to the Privacy Officer that *'it was not done with any malicious intent, merely curiosity'* and that you *'just looked and did not record or even remember anything'* from these records, the Confidentiality Booklet relevantly states that you do not have to disclose the information to someone else, just looking at a customer or employee's record when you are not authorised is an offence under various legislation Centrelink administers.

34. Based on the evidence contained in the Privacy Incident Investigation Report, it is my conclusion that you did access your own Centrelink customer record and those of seven (7) of your family members, and you knew, or ought to have known, that in the circumstances:

    a. your conduct was unauthorised and a breach of Centrelink policy;

    b. your conduct represented a failure to comply with Social Security legislation concerning authorised access to information; and

    c. your conduct constituted a conflict of interest, and it was incumbent upon you to take steps to avoid that conflict of interest.

CONDUCT CONSTITUTED A BREACH OF THE CODE OF CONDUCT

35. Having regard to all of the evidence, I have formed an opinion that your conduct was in breach of the APS Code of Conduct. A discussion of this finding in relation to each of the elements of the Code follows.

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

36. Centrelink employed you in a position of trust. Centrelink trusted and required you to comply with the 'unauthorised access' rules and inform other Centrelink staff of any circumstance in which a conflict of interest might arise. You knew, or should have known, that you should not have accessed records or processed any activities for yourself, your family and/or acquaintances. You also knew, or should have known, to inform your Team Leader/Senior Officer or Privacy Officer if you inadvertently accessed such records. It appears that you chose not to abide by Centrelink's clear directions to you about how you were to behave. I regard your behaviour as displaying a fundamental lack of honesty and integrity.

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

37. Your failure to comply with Centrelink's 'unauthorised access' rules represents a serious shortcoming in the performance of your basic duties. The fact that you have been reminded on many occasions about the 'unauthorised access' rules and your duty to take steps to avoid conflicts of interest reinforces the extent of your shortcomings. I find that your conduct demonstrated a lack of care and diligence in the performance of your duties.

(4) An APS employee must comply with applicable Australian laws

38. Your failure to comply with Centrelink's 'unauthorised access' rules led you to fail to comply with applicable Australian laws, specifically a failure to comply with the social security laws about accessing, using, recording and disclosing protected customer information described under the heading 'Legislation/Policies/Instructions', above. I make no finding that you are guilty of an offence under the applicable provisions, but I am satisfied on the balance of probabilities that you did not comply with those provisions.

(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.

39. The Chief Executive's Instructions referred to in this report set out a series of lawful and reasonable directions, which for the sake of convenience I have described in this report as Centrelink's 'unauthorised access' rules. I find that your failure to comply with Centrelink's 'unauthorised access' rules breached this aspect of the Code of Conduct.

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

40. As noted above, I am satisfied that you did not disclose the conflict between your personal connections with the people whose records you accessed and your duty as a Centrelink employee not to access your own Centrelink customer record or those of your family members. Nor did you take any steps to avoid the apparent conflict. I am satisfied that you have breached this aspect of the Code of Conduct.

(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.

41. I am satisfied that your conduct, particularly your ongoing pattern of disregarding Centrelink's 'unauthorised access' policies, represents a failure to uphold the APS Values, which are set out in section 10 of the 1999 Act.

42. In particular, I consider that in behaving as you did, you failed to uphold the APS Value that provides *'the APS has the highest ethical standards'*. Ethical conduct, in this situation, demanded that you not access your own Centrelink customer record or those of your family members at all. You did not behave in this way and thus demonstrated a failure to behave ethically in relation to those records.

SANCTION

43. In considering what sanction to recommend, I am mindful of the fact that the imposition of a sanction is for the purposes of protecting the APS and deterring similar conduct

and not for the purpose of punishment (although the imposition of a sanction may be detrimental to an employee).

44. I note that you are 47F years of age and have worked in Centrelink since 11 August 2008. I note that you presently work as a Customer Service Advisor in the S 47F As an employee whose duties require regular access to Centrelink customer records, I consider that you have a high degree of responsibility to treat those records in an appropriate way. I regard the fact that you failed to do so as very serious.

45. I note that you have failed to comply with Centrelink's 'unauthorised access' rules on thirteen (13) separate occasions over a period of 10½ months. Your actions related to your own Centrelink customer record and those of seven (7) of your family members.

46. Whilst your actions demonstrate a disregard for Australian Law and organisational policy, they first occurred at a time when you had only approximately four (4) months experience working in Centrelink and at a time when you were only being paid at the Centrelink band 2 level 01 (APS 3). I believe your lack of experience in Centrelink at the time of the unauthorised accesses could be considered a mitigating circumstance.

47. I note that you only made unauthorised access to customer records and apparently did not use or disclose information you obtained. The fact that no-one outside of Centrelink knew, or is likely to have known, of your misconduct is not regarded as a mitigating factor, but rather as the absence of an aggravating factor. Your misconduct will not be regarded as less serious merely because it remained hidden from public view.

48. In light of the fact that you have browsed a number of records over a prolonged period, it seems clear that you have persistently ignored Centrelink's rules, including the 'unauthorised access' rules. I regard your current misconduct as quite characteristic and wholly unacceptable. It demonstrates a complete disregard for Centrelink's 'unauthorised access' rules. It seems clear to me that notwithstanding any sanction applied, you could possibly repeat your unacceptable behaviour if the opportunity and desire arose. I regard this as a weighty aggravating factor.

49. In your statement to the Privacy Officer, you explained that *'there is no reason for what I have done, it was completely wrong of me to have accessed these records'*. You added that *'I underestimated the seriousness of breaching the privacy rules, and for this I apologise deeply and vow to never do anything like this again, and to always adhere to the APS code of conduct'*. I conclude that you genuinely regret your actions and believe that you have learned a lot about your responsibilities as a result of this investigation. This learning is a positive outcome for you and for Centrelink. I believe that your admission of your actions and your remorse are mitigating factors in this instance.

50. Having considered the evidence, facts and mitigating and aggravating circumstances of this case, and in accordance with section 15 of the *Public Service Act 1999*, I recommend that the sanction of deductions from salary, by way of a fine of $800.00, be applied.

51. I am of the opinion that this sanction is appropriate in the circumstances as it aims to ensure the integrity of Centrelink's data is protected and provides you with an understanding that Centrelink takes situations involving unauthorised access to protected information very seriously. An officer with over eighteen (18) months

experience, you have been employed by Centrelink during a period of heightened privacy awareness in Centrelink. The aforementioned staff instructions and policies have been supported by training programs at various times. Records indicate that you attended a Privacy Awareness Session at S 47F on 19 August 2008. On 13 August 2008, you were also provided with a "Declaration of Confidentiality" booklet, which outlines employees' privacy and confidentiality responsibilities and includes a declaration that employees will undertake to read and abide by the policies contained within. You signed this declaration on 13 August 2008. On 19 August 2008 and then again on 12 August 2009, you also electronically acknowledged Declarations of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities. I conclude that you have, therefore, been regularly made aware of your privacy and confidentiality responsibilities in a variety of different ways, and yet on a number of occasions, chose to ignore them.

52. I considered that a reprimand was too lenient a sanction, as I believe your breaches of the Code of Conduct were serious, and committed with full knowledge of Centrelink's policies relating to Privacy and Confidentiality. The Australian public needs to have a high level of trust in Centrelink's ability to manage and protect personal information. Your unauthorised accesses to protected information are very serious in that they compromise our ability to maintain public confidence in these aspects of public service. The protection and management of customer information is at the core of the everyday business activities of the majority of Centrelink's employees, and any actions which impact on our ability to guarantee privacy and confidentiality to customers must be viewed as grave offences. Further, your actions have clear potential impacts on the reputation and standing of Centrelink in the community. The prohibitions on staff conduct exist both to ensure and to maintain the appearance of fair and ethical professional conduct. Your actions have the potential to erode both of these aspects of public confidence in Centrelink.

53. I have no confidence that if a lesser sanction were applied under subsection 15(1) of the *Public Service Act 1999*, you would not again misuse Centrelink records in future, if it suited you to do so. In searching for your own Centrelink customer record and those of family members, you failed to act in accordance with Centrelink policy, despite by your own admission, recognising that your personal connection to the customers in question meant that you were not authorised to access their records. I therefore do not consider that a lesser sanction would be an adequate response to the gravity of your conduct.

54. As all employees in Centrelink are required to comply with Centrelink's 'no browsing' rules, I am not satisfied that such breaches would be less likely to occur were you moved to work in a different program area, a different office, or a different role. I therefore do not believe that reassignment of duties is an appropriate sanction in this instance.

55. Finally, I considered that the sanctions of demotion and termination of employment were too harsh. Your unauthorised accesses appear to be primarily for the purpose of browsing. Whilst these accesses were unauthorised, they do not appear to have been made for the purpose of obtaining a benefit or an advantage for yourself or any other person. In light of the statement that you provided to the Privacy Officer, I conclude, on balance, that your awareness of Centrelink's 'unauthorised access' rules will develop and improve as a result of this process and you will become very aware of your

obligations. I therefore believe that it is extremely unlikely you will commit a breach of privacy at any time in the future.

56. I have therefore decided on deductions from salary, by way of a fine of $800.00, as the most appropriate sanction. It represents a significant sum of money and thereby reflects the gravity of this offence.

s 47F

Professional Standards Officer
People Support Team
s 47F

9 March 2010