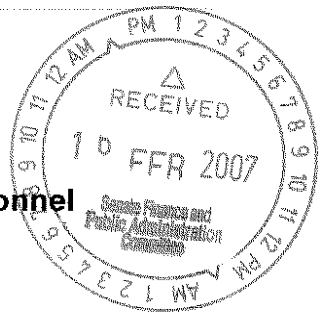
Financial Management & Business Support Division

Financial Management & Services Branch



Chief Executive Instructions

Version Control # 2006-002

20. Unauthorised Access to Centrelink Customer Records and the Personnel Records of Centrelink Officials.

Summary

This CEI:

is to clearly articulate Centrelink's rules regarding unauthorised access to the personal information of Centrelink customers and employees.

Notes

a. This instruction applies to the personal information of Centrelink customers and employees contained in either paper or computer records.

b. These instructions are in place to protect employees from unfounded allegations regarding unauthorised access to personal information and to protect the privacy of our customers and employees.

Unauthorised Access

Centrelink employees are given access to the personal information of customers and employees in order for them to carry out their prescribed duties. Accessing the paper or computer record of a customer or employee without authorisation is commonly referred to as **'browsing'**. Unauthorised access includes browsing, processing transactions and completing activities within the records of customers or employees where there is no legitimate business reason to do so or where Centrelink has determined that an employee must not access the records without specific authorisation from a team leader/manager. Refer to section **3.060** of the Privacy and Confidentiality Manual.

Conflict of Interest

Under the Australian Public Service (APS) Code of Conduct as contained in subsection 13(7) of the Public Service Act 1999, Centrelink employees must disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with their employment. This restriction does not apply to everyone the 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/disadvantage in his or her dealings with Centrelink. It is recognised, particularly in small communities, that an employee cannot be removed from handling every case where he or she knows the customer personally. Refer to section 3.060 of the Privacy and Confidentiality Manual.

Inadvertent access

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 notify their team leader/manager and explain the situation. The team leader or manager must make a note of the inadvertent access in a secure office register. For further information regarding inadvertent access refer to section **3.100** of the Privacy and Confidentiality Manual.

Instructions

20.01(ii)	There would be a **conflict of interest**, and therefore a potential breach of the APS Code of Conduct, where a Centrelink employee has a personal interest in the customer or employee whose record is being accessed. For this reason, except in circumstances outlined in CEI 20.02, a Centrelink employee must not access the information or records of the following: • themselves; • their family members; • their relatives, including in-laws; • their ex-partner and ex-family members; • neighbours; • their friends or emergency contacts; • their close personal acquaintances; or • their work colleagues **(Refer CEI 21).** Refer section **3.063** of the Privacy and Confidentiality Manual. An employee can use their work computer to access their customer record via the external Centrelink **Internet** website Customer Online Services option. However, they must NOT use the Customer Online view to access their own customer record. Centrelink employees are authorised to access their own **Infolink** record on the Intranet.
20.02(ii)	The Team Leader/Manager can authorise access to a customer's record or a Centrelink employee's personnel record where there is a 'conflict of interest' provided it is an operational necessity and alternative options do not exist. In this situation, the **Team Leader/Manager must**: • where a customer record is accessed, record an 'AAA' enquiry type DOC on their record. The 'AAA' enquiry type DOC automatically records the log-on ID of the authorising Team Leader/Manager when it is applied. The Team Leader/Manager is required to enter into the 'AAA' enquiry type DOC the authorised employee's log-on ID details and the date of the access they are approving; or • in the case of an access to an employee's personnel record, attach a signed file note on that employee's personnel file. If a Centrelink employee has any doubts about a situation, they should consult their Team Leader, Manager or Area Privacy Officer for advice. Refer section **3.071** of the Privacy and Confidentiality Manual.
20.03(ii)	A customer cannot authorise an employee to access the customer's record where such an access would be contrary to Centrelink practices for handling conflict of interest situations. Refer section **3.072** of the Privacy and Confidentiality Manual.
20.04(ii)	Where a Centrelink employee has permission to enquire on behalf of a customer or is a nominee for a customer they must **not** access the individual's record. Refer **CEI 21**.

Further information regarding these topics is in the Privacy Awareness Kit available online.

References

Unauthorised accesses are considered breaches of the following legislation and instructions:

- APS Code of Conduct, section 13 of the *Public Service Act 1999*;
- Confidentiality provisions contained in various legislation administered by Centrelink including:
- sections 203 and 204 of the *Social Security (Administration) Act 1999*;

- sections 163 and 164 of the *Family Assistance (Administration) Act 1999*;
- Information Privacy Principle 4 of the *Privacy Act 1988*;
- Chapter 3 of the Privacy and Confidentiality Manual which details policy in relation to the storage and security of personal information;
- Centrelink's 'Declaration of Confidentiality/Security and Privacy Responsibilities' booklet which includes the 'Rules for the Handling of Personal/Protected Information'; and
- National Call Centre Procedures to Follow When a CSA Inadvertently Accesses a Customer's Record.

Breaches

A Centrelink employee found to have breached the APS Code of Conduct may have one or more of the sanctions, as prescribed in section 15 of the *Public Service Act 1999*, imposed.

A Centrelink employee making unauthorised access to a customer record may also face criminal charges under the confidentiality provisions contained in various legislation administered by Centrelink.

Contacts

The business owner of this CEI is:

National Manager
Legal Services Branch

The contact is:
Joan Savic
Spectrum 120310

Date of Effect

18 December 2006

Chief Executive Officer Authorisation

Dated this 18th day of December 2006

Jeff Whalan

Chief Executive Officer

Commonwealth Services Delivery Agency

top