



# PUBLIC TRUSTEE AND GUARDIAN POLICY

DOCUMENT PROPERTIES	
Name of Policy	Information Security
PTG Policy Number	2017-6
Version/s	30.11.2016
Endorsed by SLG	30.11.2016
Authorised by	Andrew Taylor, Public Trustee and Guardian
Date for review (plus three years)	30.11.2016

## LEGISLATION

S 9(m)(i)&(ii) of the *Public Sector Management Act 1994* provides that the public employee shall not disclose, without lawful authority, any information acquired by him or her as a consequence of his or her employment or any information acquired by him or her from any document to which he or she has access as a consequence of his or her employment.

Shared Services ICT Policy Version 2.4, September 2014 establishes the information security regulatory framework for information being processed in electronic form for the ACT Government.

S 65A of the *Public Trustee and Guardian Act 1985* provides that it is an offence to use, disclose or do something to disclose protected information unless authorised under the Act, in a Court proceeding or with the protected person's consent.

JACS Security Management Clear Desk Policy requires that all classified or sensitive material (including portable and attractive items e.g. laptops and PDAs) are secured in the appropriate container when the room is unattended and upon completion of the day's work.

## DEFINITION/S

**Information security** - is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

**Protected information** - means information about a person that is disclosed to, or obtained by, an information holder because of the exercise of a function under this Act by the information holder or someone else.

**Court** - includes a tribunal, authority or person having power to require the production of documents or the answering of questions.

**Disclose** - includes communicate or publish.

**Information** - means information, whether true or not, in any form and includes an opinion and advice.

## **POLICY**

Information security should be a priority of all staff in undertaking their duties and may include but is not limited to:

- ensuring that any faxes containing personal information are sent to the correct fax number;
- ensure current consent authorisation is current for all clients under your management;
- ensuring that client possessions are not left around the office;
- disposing of classified and personal information in the appropriate recycling bin;
- never share your password;
- log off your PC every night;
- do not discuss client details with anyone outside of the office unless that discussion is in the course of business and is necessary;
- if you are the last to leave the office at the end of the day, ensure that the strong room is locked and office is alarmed upon departure;
- adopt a clear desk policy and don't leave client files or papers on your desk when you leave for the day;
- never discuss anything with the media, Ombudsman & MLA's (whether government or non-government) - direct all such enquiries to your Manager or to the Public Trustee and Guardian;
- ensure that visitors are signed in and a visitors card issued; and
- report any security incidents to senior management.

**END OF POLICY**