

Privacy Knowledge Site - Introduction

This, and the following pages, have been developed to provide people with an understanding of the Australian Privacy Principles (APPs) and how they are to be applied in the Defence context.

This information should provide you with sufficient information to successfully complete the APP: e-Assessment CAMPUS course (Campus ID# 7392). It is also a resource which can be used at any time and should be the initial resource referred to when dealing with privacy related issues.

Information about each Australian Privacy Principle can be accessed by hovering over the 'Privacy' tab on the menu at the left of the screen.

The Privacy Act 1988

The [Privacy Act 1988](#) (the Privacy Act) provides the conditions under which government agencies and organisations may collect and handle personal information. These conditions used to be known as the Information Privacy Principles, but were replaced by the Australian Privacy Principles on 12 March 2014.

The Privacy Act also provides 'Permitted General Situations' which are exceptions to the general limitations on the collection, use and disclosure of personal information. Information about the permitted general situations can be found on the '[permitted general situations](#)' page.

Before looking at the Australian Privacy Principles, you should look at the '[Important terms](#)' page. These will help your understanding of the Privacy Act, as several words have particular meanings when used in a privacy context.

The Australian Privacy Principles


Defence is required to comply with the Australian Privacy Principles which are contained in Schedule 1 of the Privacy Act. There are 13 Australian Privacy Principles and they are commonly referred to as the APPs. Of the 13 principles, only 11 apply to Defence. The Australian Privacy Principles are structured as follows.

PART 1 – Consideration of personal information APPs 1 & 2
PART 2 – Collection of personal information APPs 3 to 5 Formally IPPs 1, 2 & 3
PART 3 – Dealing with personal information APPs 6 to 9* Formally IPPs 10 & 11
PART 4 – Integrity of personal information APPs 10 & 11 Formally IPPs 3, 4, 8 & 9
PART 5 – Access to, and correction of, personal information APPs 12 & 13 Formally IPPs 6 & 7

* APPs 7 & 9 do not apply to Defence

Australian Privacy Principle guidelines

The Office of the Australian Information Commissioner (OAIC) has published guidelines to assist in the interpretation and understanding of the Australian Privacy Principles. The guidelines supplement the information provided on this site and will provide you with a more in-depth understanding of the Australian Privacy Principles, but without the Defence context.

The guidelines contain detailed information on how to interpret the APPs. A copy of the OAIC APP guidelines document can be viewed by clicking on the following link:  [OAIC-APP-guidelines pdf](#)

Interference with an individual's privacy

The Office of the Australian Information Commissioner (OAIC) refers to a breach of a person's privacy as an 'interference'.

If Defence is found to have breached the APPs, by unlawfully using or disclosing an individual's personal information, the OAIC refers to the breach as an interference with that individual's privacy. The OAIC has the power to impose financial penalties on an agency in response to breaches of the Privacy Act.

In accordance with the Privacy Act, only APP entities can be penalised by the OAIC for breaching a person's privacy. However, individual Defence personnel can be sanctioned, disciplined or referred to Code of Conduct (which ever is the appropriate internal mechanism), under a breach of the Defence Security Manual (eDSM) or an applicable Defence Instruction, for mishandling personal information.