

Contents

Statement	6
Section 1: Introduction	7
Australian Privacy Principles	7
Overview of the APPs	7
Are RTOs covered by the APPs?	8
Small business operator	9
Applying these definitions to RTOs	9
What happens if an APP entity breaches an APP?	9
Using this Guide	10
APP Awareness Presentation	10
Section 2: Summary of the Key Changes	11
What Do the APPs Mean for RTOs?	13
Section 3: APP Guidelines for RTOs	16
Australian Privacy Principle 1 – Open and transparent management of personal information	16
Reasonable Steps	16
Developing an APP Privacy Policy	17
Information that must be included in an APP Privacy Policy	17
Making an APP Privacy Policy publicly available	19
Australian Privacy Principle 2 – Anonymity and pseudonymity	20
Anonymity	20
Pseudonymity	20
Providing options	21
Requiring identification – required or authorised by law	21
Requiring identification – impracticability	21
Australian Privacy Principle 3 – Collection of solicited personal information	22
‘Solicit’ and ‘collect’	22
Collection for a RTO’s ‘functions or activities’	23
Collecting sensitive information	23
Collecting by lawful and fair means	24
Collecting directly from the individual	25
Australian Privacy Principle 4 – Dealing with unsolicited personal information	26
What is ‘unsolicited’ personal information?	26
Could unsolicited personal information have been collected by the RTO under APP 3?	27
Dealing with unsolicited personal information	27
Deal with unsolicited personal information that is not destroyed or de-identified?	28
Australian Privacy Principle 5 – Notification of the collection of personal information	29
Reasonable steps to notify or ensure awareness	29
Matters to be notified	30
When notification is to occur	32

Australian Privacy Principle 6 – Use or disclosure of personal information.....	33
‘Hold’, ‘use’, ‘disclose’ and ‘purpose’.....	33
‘Purpose’ of collection.....	34
Use or disclosure for a secondary purpose.....	34
Using or disclosing personal information as required or authorised by law.....	36
Using or disclosing personal information where a permitted general situation exists.....	36
Using or disclosing personal information for an enforcement related activity.....	36
Related bodies corporate.....	37
Australian Privacy Principle 7 – Direct marketing.....	38
What is direct marketing?.....	38
When are agencies covered by APP 7?.....	39
Providing a simple means for ‘opting out’.....	40
Using and disclosing personal information for the purpose of direct marketing where no reasonable expectation of the individual, or information collected from a third party.....	40
Consent.....	40
Requests by an individual to stop direct marketing communications.....	41
Requests by an individual to stop facilitating direct marketing.....	42
Interaction with other legislation.....	42
Australian Privacy Principle 8 – Cross-border disclosure of personal information.....	43
What is an overseas recipient?.....	43
When does a RTO ‘disclose’ personal information about an individual to an overseas recipient?.....	43
When will a RTO have taken reasonable steps?.....	44
Disclosure of personal information to an overseas recipient that is subject to a similar law or binding scheme.....	45
Disclosure of personal information to an overseas recipient with the individual’s consent after being expressly informed.....	46
Disclosure of personal information to an overseas recipient as required or authorised by law.....	46
Disclosure of personal information to an overseas recipient where a permitted general situation exists.....	46
Disclosure of personal information to an overseas recipient for an enforcement related activity.....	47
When is a RTO accountable for personal information that it discloses to an overseas recipient?.....	47
Australian Privacy Principle 9 – Adoption, use or disclosure of government related identifiers.....	48
What is a ‘government related identifier’?.....	48
When are agencies covered by APP 9?.....	49
Adoption of government related identifiers.....	49
Use and disclosure of government related identifiers.....	49
Australian Privacy Principle 10 – Quality of personal information.....	51
What are reasonable steps?.....	51
What are the quality considerations?.....	52
Australian Privacy Principle 11 — Security of personal information.....	54
When does a RTO ‘hold’ personal information?.....	54
What are reasonable steps?.....	54
What are the security considerations?.....	55

Destroying or de-identifying personal information.....	56
Australian Privacy Principle 12 — Access to personal information	58
‘Holds’.....	58
Access to ‘personal information’.....	58
Verifying an individual’s identity	59
Giving access under APP 12 – processing requirements.....	59
When a RTO may refuse to give access under APP 12	60
APP 12 minimum access requirements	60
Access Charges	62
Giving written notice where access is refused, or not given in the manner requested under APP 12	62
Australian Privacy Principle 13 – Correction of personal information	64
When a RTO must take reasonable steps to correct personal information.....	65
Grounds for correcting personal information	66
Being satisfied and taking reasonable steps.....	66
Reasonable steps to notify another organisation	67
APP 12 minimum procedural requirements.....	67
Section 4: Implementing the APPs in your RTO	69
Privacy Impact Assessment (PIA).....	69
What is a PIA?.....	69
Why do a PIA?.....	69
Conducting the PIA.....	69
Example PIA Tool.....	71
APP Compliance Checklist	71
APP Action Plan.....	71
Section 5: Further Resources & Information	72
Further Resources & References	72
Further Information.....	72
Appendix A: Australian Privacy Principles in Detail.....	73
Part 1—Consideration of personal information privacy.....	73
Part 2—Collection of personal information.....	74
Part 3—Dealing with personal information	76
Part 4—Integrity of personal information.....	79
Part 5—Access to, and correction of, personal information	80
Appendix B: Example Privacy Impact Assessment Tool.....	83
Appendix C: Example APP Compliance Checklist for RTOs	89
Appendix D: Example APP Privacy Policy for RTOs.....	103
‘Request for Records Access’ Procedure	111
‘Request for Records Update’ Procedure	112
Privacy Complaints Procedure.....	113
Appendix E: Example APP Tools for RTOs	114

APP Action Plan	114
APP Notice	115
Retention and Disposal Schedule	116
Records Access or Update Request Form	117
Records Access Request – Refusal Notice	118
Records Update Request - Refusal Notice	119
Data Breach Response Plan.....	120
When a data breach occurs.....	120