



## Appendix H: Privacy Policy

### 1. Introduction

On 21 December 2001, amendments were made to the *Commonwealth Privacy Act 1988* which apply to the private sector, including private providers of Education and Training such as Raffles College. The amendments oblige Raffles College to handle personal information in accordance with 10 National Privacy Principles. These principles cover the collection, storage, use and disclosure of personal information. They also give people a right to seek access to the personal information that organisations hold about them. The legislation affects Raffles College in a number of ways, especially student rights and public access.

The *National Privacy Principles* cover the collection, storage, use and disclosure of personal information. They also give people a right to seek access to the personal information that organisations hold about them. Other Commonwealth and State legislation with which we must comply also determine to some extent what information we collect and how it is handled. Information collected about overseas students must also comply with the *Commonwealth Education Services for Overseas Students (ESOS) Act 2000*.

Raffles College has security systems in place to protect all the information we handle from misuse and unauthorised disclosure or modification, and we do not retain data for which we have no further use, except where required by statute to preserve student *academic* records for thirty years. Requests for access must be in writing, and we may charge a fee to cover administration costs. If anyone has any questions about our privacy policy, or if anyone wants to see, correct, or find out about the personal information we hold about a person, please contact our Registrar on (02) 9922 4278 or at [contact@raffles.edu.au](mailto:contact@raffles.edu.au)

For details about the Commonwealth Privacy Act, please contact the federal Privacy Commissioner on 1300 363 992 or visit the appropriate website - <http://www.privacy.gov.au>

### 2. Background

A paper entitled 'Privacy Law for Providers of Education and Training' authored by Lindy Smith, Director of Privacy management, was presented at the ACPET Privacy Seminars held in the eastern states in November-December. She is an expert in the area, having worked for the Privacy Commissioner and she was involved in the drafting of the new Privacy Law. The following comments are extracted from that paper.

The Commonwealth Parliament has extended the coverage of the *Commonwealth Privacy Act 1988* to encompass more of the private sector. Those brought under the legislation were given at least 12 months to prepare, so time is running out. The new law came into effect for them from 21 December 2001.

The Privacy Act 1988 was passed in the wake of the Australia Card debate to assure the public that the Commonwealth Government could be trusted with the personal information it collects. Attached to the Act were guidelines on handling Tax File Numbers. Almost immediately, it began to be tinkered with in response to isolated issues, such as access to information about old criminal convictions, the conduct of data matching, the handling of some health data and the privatisation of some government services. Until last year, the most significant amendment was in 1990, when the Act was expanded to cover consumer credit reporting activities.

During the 1990s, the focus of debate about privacy moved from government activities to the impact of new communications and information technology throughout the community. Surveys revealed a high level of anxiety among Australians about the amount of personal information being collected and used without their knowledge or consent. This was recognised as a barrier to e-commerce in particular and the take-up of new technology generally. A global dimension was added when the European Union decided to prohibit the transfer of personal information about its citizens to foreign destinations that do not protect privacy to an adequate standard. Meanwhile, the Commonwealth government was privatising and outsourcing its activities, blurring the line between the public and private sectors and effectively reducing the coverage of the Privacy Act. Inquiry after inquiry found the best solution would be to extend privacy legislation to the entire private sector. By the March 1996 election, all major political parties were promising to do this.

The new federal government's first proposal was to have a comprehensive privacy law, which it outlined in a discussion paper that the Attorney-General released in September 1996. Within six months, it had abandoned the idea completely. Many more false starts, protracted negotiations, inquiries and reviews later, the new legislation was finally passed in December 2000. Compared to the original proposal, the law is more modest in scope but greater in volume. Even as he tabled it in Parliament, the Attorney-General promised that it would be reviewed in two years' time. Any changes in the future are unlikely to do other than increase its coverage.

### **3. Who Must Comply**

The Act does not cover the entire private sector. It applies only to organisations undertaking activities that represent, in the government's view, the greatest risk to privacy. The line of demarcation is a wobbly one. Most have had to comply by 21 December 2001. However, small businesses other than health service providers have until 21 December 2002 to prepare.

### **4. Protecting 'Personal Information'**

The Privacy Act regulates the way that private sector organisations handle 'personal information'. Personal information is information or opinion that can identify a person either directly or indirectly and is recorded in some form.



The Act also recognises that some types of personal information are more sensitive than others. 'Sensitive information' is personal information about a person's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, or 'health information'. 'Health information' is also defined in a particular way in the Act. It includes information about a person's health or disability at any time, the health services they have received in the past or wish to receive in the future, all personal information collected in providing a health service, and other personal information collected in connection with the donation of body parts, organs or substances.

## 5. The National Privacy Principles

Organisations covered by the new law will have to handle personal information in accordance with ten National Privacy Principles (NPPs). In essence, the NPPs aim to ensure that personal information is used and disclosed only for the primary purpose for which it was collected, unless otherwise authorised by the person or by law. They regulate the handling of personal information from collection to destruction and can be summarised as follows.

- (a) *Collection* — collect only what is necessary, collect it fairly and lawfully, collect it from the person if possible, and let them know why it is collected and to whom it might be disclosed (applies only to information collected after the Act comes into effect)
- (b) *Use and disclosure* — use and disclose personal information only for the primary purpose for which you collected it unless you get the person's consent or one of the other exceptions set out in NPP 2 applies (applies only to information collected after the Act comes into effect)
- (c) *Data quality* — take reasonable steps to ensure the personal information you use is accurate, complete and up to date (applies to existing information that is used after the Act comes into effect, plus all information collected after that date)
- (d) *Data security* — take reasonable steps to protect the personal information you hold from misuse and unauthorised access, disclosure and modification; destroy or de-identify that which you don't need any more (applies to information collected at any time)
- (e) *Openness* — be open about what sort of personal information you hold and your information management policies (applies to information collected at any time)
- (f) *Access and correction* — provide the person with access to personal information you hold about them, and the opportunity to correct it if necessary, subject to exceptions listed in NPP 6 (applies to existing information that is used after the Act comes into effect, plus all information collected after that date)
- (g) *Identifiers* — do not adopt, use or disclose an identifier assigned by a Commonwealth government agency unless authorised to do so (applies to information collected at any time)
- (h) *Anonymity* — give individuals the option of not identifying themselves wherever this is lawful and practicable (applies only to information collected after the Act comes into effect)



- (i) *Transborder data flows* — do not transfer personal information overseas unless you expect it to be protected to a similar standard, the person consents or the transfer is in the person's interests (applies to information collected at any time)
- (j) *Sensitive information* — do not collect sensitive personal information (as defined in the Act) unless with the person's consent or as authorised by one of the exceptions in NPP10 (applies only to information collected after the Act comes into effect)

## 6. Codes

Instead of complying with the National Privacy Principles, organisations or industries may prepare and enforce their own codes. If approved, a code replaces the principles for the organisations that are bound by it. Conditions apply, including those listed below.

The public must have been given an adequate opportunity to comment on a draft of the code

The code must contain obligations that are at least the equivalent of those in the National Privacy Principles overall

It must comply with guidelines that the Privacy Commissioner has issued.

It can establish its own complaint mechanism, which must provide for an independent code adjudicator who can exercise powers similar to the Privacy Commissioner but is required to report to him annually about the complaints handled and how they were resolved

Alternatively, the Privacy Commissioner can be the independent code adjudicator

The Privacy Commissioner must approve the code.

## 7. Complaint Handling

People who believe that an organisation has not been handling their personal information in accordance with the National Privacy Principles or an applicable code will be able to make a complaint. They will need to approach the organisation first, which should try to resolve the problem through negotiation. If this fails to produce a satisfactory solution, the person can refer the complaint to either the Privacy Commissioner or an independent code adjudicator. Decisions by a code adjudicator can be reviewed by the Privacy Commissioner at the complainant's request. Decisions by either the Privacy Commissioner or a code adjudicator can be enforced in the Federal Court or the Federal Magistrates Service.

## 8. The Role of the Privacy Commissioner

The Privacy Commissioner is Malcolm Crompton. His role is specified in the legislation (s27). It includes:

Providing policy advice and guidelines

Approving privacy codes

Hearing complaints

Investigating breaches of the Act (whether or not a complaint has been made)

Conducting audits of government agencies

On request, examining the practices of private and non-government organisations



Undertaking research

Promoting the privacy principles in the wider community.

## **9. Conclusion**

The best single source of information about the law and how to comply with it is the Federal Privacy Commissioner's website: [www.privacy.gov.au](http://www.privacy.gov.au)

For more specific ideas about the impact of privacy laws on education providers, keep in mind that NSW government organisations operate under the NSW Privacy and Personal Information Act 1997, which is based on Information Protection Principles that are very similar to the National Privacy Principles. See the NSW Privacy Commissioner's website: [www.lawlink.nsw.gov.au/pc.nsf](http://www.lawlink.nsw.gov.au/pc.nsf)

