

# Privacy issues in online teaching and learning

Australian Flexible Learning Framework Quick Guides series

Based on the knowledge generated from the Australian Flexible Learning Framework projects and selected external literature, the Quick Guides series provides an introduction to key issues related to flexible and online delivery of Vocational Education and Training (VET).

Reference as:

Backroad Connections Pty Ltd 2003, *Privacy issues in online teaching and learning* (Version 1.00), Australian Flexible Learning Framework Quick Guides series, Australian National Training Authority.

Version 1.0~~1~~, ~~2~~ July 200~~4~~

This document can be accessed at:  
<http://flexiblelearning.net.au/guides/privacy.pdf>

For a list of other Quick Guides see:

<http://flexiblelearning.net.au/projects/sharingknowledge.htm#guides>

Deleted: 0

Deleted: 29

Deleted: 3

Field Code Changed

Deleted: <http://flexiblelearning.net.au/guides/>

© 2003 Australian National Training Authority

This work has been produced by the Sharing Knowledge project with the assistance of funding provided by the Commonwealth Government through the Australian National Training Authority. Copyright for this document vests in ANTA. ANTA will allow free use of the material so long as ANTA's interest is acknowledged and the use is not for profit.

The views and opinions expressed in this document are those of the authors and do not necessarily reflect the views of ANTA. ANTA does not give any warranty or accept any liability in relation to the content of this document.

*An initiative within the Australian Flexible Learning Framework for the National Vocational Education and Training System 2000-2004*

*Managed by the Flexible Learning Advisory Group on behalf of the Commonwealth, all States and Territories in conjunction with ANTA*

## Scope

This Quick Guide discusses privacy issues specific to online teaching and learning. It assumes that you are operating in an organisation such as a Registered Training Organisation (RTO) or under the auspice of a state training authority that is required to have a privacy policy.

Most privacy advice is ultimately a matter of legal interpretation, and is dependant upon many factors, including governing State legislation, hence it is only possible to provide general legal information in this guide. The intention of this guide is to alert you to issues and activities in relation to online teaching and learning which may raise privacy implications. Ultimately decisions about policy will need to be made by people in your organisation with authority and knowledge to make such decisions based on legal advice specific to your situation. This guide can help you identify issues which need to be considered and direct you to additional resources.

This guide does not cover other related issues such as freedom of information, defamation, discrimination, copyright, and telecommunications (including privacy issues under telecommunications legislation). For these areas refer to the *Legal issues in flexible learning* project at <http://flexiblelearning.net.au/projects/legalissues.htm>

Deleted: <http://flexiblelearning.net.au/legal/>

## Aspects of privacy law

### What is covered by privacy law

“Privacy law covers personal information and records containing personal information. Personal information means any information or opinion, true or not, about an identified or identifiable individual. A record could be a document, database, film or photograph.” (Resources booklet, Legal issues in flexible learning Information Kit)

### Is my organisation subject to privacy law?

Privacy law includes:

- The Federal Privacy Act, which contains eleven Information Privacy Principles (IPPs) which apply to Commonwealth and ACT government agencies. It also has ten National Privacy Principles (NPPs) which apply to parts of the private sector (business and not-for-profit) and all health service providers.
- Various state and territory legislation.

Different privacy rules may apply to different organisations. For example, if an organisation is funded/controlled by the Commonwealth, the Federal Privacy Act and Information Privacy Principles may apply to that organisation. Otherwise, the private sector privacy obligations may apply (National Privacy Principles), and there are also State and Territory privacy laws which may also impose obligations on an agency. The first step is therefore to identify which rules apply to your organisation. Defining this is beyond the scope of this guide and organisations will need to get legal advice as to which privacy legislation they must comply with.

However it is good practice for all organisations to comply with the National Privacy Principles (NPPs) of the Federal Act, the essence of which are summarised below.

For more information on state and territory legislation refer to the page at:  
[http://www.privacy.gov.au/privacy\\_rights/laws/index.html](http://www.privacy.gov.au/privacy_rights/laws/index.html)

## The National Privacy Principles

Schedule 3 of the Privacy Act sets out the ten National Privacy Principles (NPPs), which legally bind organisations covered by the Act in the way they must handle personal information. These cover:

- **Collection** (NPP 1) includes that the collection must be necessary, done by lawful and fair means and not in an unreasonably intrusive way and that the individual is aware of the collection of information.
- **Use and disclosure** (NPP 2) covers how information may be used and how and to whom it may be disclosed.
- **Data quality** (NPP 3) states that “An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.”
- **Data security** (NPP 4) covers steps which must be taken to protect personal information and to destroy or de-identify it when it is no longer required.
- **Openness** (NPP 5) requires organisations to make available their policies on their management of personal information, the sorts of information they collect and how they use that information, including responding to requests about what information is held about an individual.
- **Access and correction** (NPP 6) requires organisation to provide individuals with access to information about them (with certain exemptions), requires that any charges for accessing personal information are reasonable, and that reasons are given if access to information is refused. It also addresses requirements for correction of information an individual believes is not accurate, complete or up-to-date.
- **Identifiers** (NPP 7) covers the exchange of identifiers of individuals (such as student ID numbers) between organisations.
- **Anonymity** (NPP 8) provides that “Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.”
- **Transborder data flows** (NPP 9) covers the conditions under which personal information about an individual may be transferred to someone who is in a foreign country.
- **Sensitive information** (NPP 10) covers collection of sensitive information about an individual and is particularly concerned with health information.

For further information on the National Privacy Principles refer to the page at:  
<http://www.privacy.gov.au/act/npps/index.html> and the publication *Guidelines to the National Privacy Principles* at [http://www.privacy.gov.au/publications/nppgl\\_01.html](http://www.privacy.gov.au/publications/nppgl_01.html)

## Reasons for collecting information

There are many reasons for collecting personal information. The operation of National Privacy Principles and governing privacy laws makes it important that you be clear about the reason(s) you collect specific information, because how you can use information depends on both the primary reason for which the information was collected, and what you tell people about the proposed uses at the time of collection. Reasons might include:

- **Configuring student or learning management systems:** which usually requires entering basic information about students to track their progress.
- **Research and evaluation:** consider carefully how much personal information is actually required for this purpose (as opposed, for example, to anonymous questionnaires and de-identified statistical data or examples of student work).
- **To facilitate student participation:** communication between students can be facilitated by sharing personal information.
- **To conduct transactions** (for example enrolments, payments, licences, permissions).

### Ways in which you might collect personal information

In addition to the formal collection of data for administrative or specific statistical purposes (for example student enrolment, student/course progress) there are many other ways in which your organisation might collect personal information in the conduct of online education and training. For example:

- Asking students to enter information about themselves (eg a profile page) in online conference, web-based discussion or a learning management system.
- Encouraging students to provide personal information (eg ice-breakers in online discussion).
- Recording of chat sessions.
- Automatic collection via web site statistics for whatever purpose (to the extent that these can be associated with an identifiable individual).

### Ways in which you might use personal information

There are numerous ways in which personal information might be used. Some examples which have commonly been raised in relation to flexible learning include:

- Using photos and videos of students in publications and websites (if they contain identifiable individuals).
- Providing email addresses to other students.
- Demonstrating content from your online learning systems that contains personal information about students or staff to other people (for example at a conference).
- Quoting student work in reports and evaluations.
- Publishing student work that contains names or other personal information.

## Issues

### Group pressure

Asking students to share personal information about themselves with others in their study or class group may be justifiable on pedagogical grounds and be a good teaching strategy to employ, however teachers need to be aware that some students may not wish to do this. Teachers need also to be aware of the 'power of the group' – students may feel compelled even though participation may be voluntary simply because being seen to be different alienates or distances them from the group. The thoughtful teacher might provide alternatives to make it 'OK' not to reveal more information than students feel comfortable doing. For example 'draw yourself' as an

alternative to submitting a photo; tell us about a fictitious episode, instead of a specific personal one. Encourage the sharing of information – but do be sensitive to and respectful of people's need for privacy.

### Technical infrastructure issues

Many aspects of the Internet are inherently insecure and your organisation should already have in place procedure and protocols to manage the risks inherent in connecting computer systems to the Internet. If you are establishing new online services (either using your own computers or via a service provider) you should ensure that these are covered by a management plan that covers all aspects of network security. This is beyond the scope of this guide but some examples of areas which should be covered include:

- All computers have current virus protection (viruses and related software such as Trojan program and worms can provide an avenue for unauthorised access to data on your computers).
- Firewalls are used to prevent unauthorised access.
- All hardware (but especially that containing sensitive, valuable or personal information) is physically and electronically secured.
- Procedures are in place to ensure that information about security bulletins, available patches and bug fixes for all the software used on your computer networks is monitored regularly and that updates are applied promptly.
- Data backups are securely stored.
- Suitable encryption is used when sensitive information is transmitted over the Internet.
- Your organisation provides suitable security awareness training for all staff and students.
- Secure systems are in place for the storage of personal information in electronic form.
- Appropriate levels of access management are in place and that these are enforced through good password management or other access control techniques.

For further information and links see the Federal Privacy Commissioner's Online Privacy Tools page at <http://www.privacy.gov.au/internet/tools/> which links to information and tools on firewalls, cookies, web bugs, anonymous web browsing, encrypted email, advertising filters, anti-spam tools, and further information.

### Using photographs of people

A photograph may be regarded as a 'record' that contains 'personal information' for the purposes of the Privacy Act, if the identity of the person in the photograph can be reasonably ascertained. A person's identity may be reasonably ascertained even, for example, when a photo is taken from the back or three quarters from the back (from body shape or distinctive clothing for example).

To ensure privacy regulation requirements and ethical practice are not contravened inadvertently, it is good practice to get prior written consent from any person whose photograph is to be used in printed and online material. The consent should set out all intended uses of the photograph so that no doubt arises later. If the photo is of a child you should get the consent of the child's parents before using the photo. Also, if

taking photos of people in an educational institution which has a 'duty of care' to its students, you should obtain the permission of the institution.

### **Distributing and publishing email addresses**

Email addresses of staff and students (and any other person) are likely to be regarded as personal information for the purposes of the Privacy Act, irrespective of whether the email accounts were set up by the institution or the individual.

If you wish to provide students with the email addresses of other students in a course or project you should provide information about why this information is being collected and should preferably obtain written consent.

The kinds of things that you should consider telling students might include:

- whether participation via email is a necessary part of the course or project
- that email addresses will be circulated to classmates and to specifically identified staff for the purposes of the course / project etc
- options that students might use to set up alternative email addresses so that involvement in a course does not reveal their private email address
- that students will be requested not to pass on each other's email address to persons not participating in the course / project unless that student has consented to that disclosure of their personal information
- whether the communications or comments that are made by students via email will identify them as being the author or whether the contributions will be de-identified.

The safest course of action will always be to obtain the individual's consent for the collection and intended use or disclosure of their personal information. If you are in any doubt as to how well informed existing students are about use of their email address, or if you are setting up a new initiative, then you should consider obtaining the students' written consent. This need not be a complicated process – just a simple acknowledgment by the student (preferably in writing) that they understand the purposes for which their email address is to be collected, used and disclosed (shared). This could be in the format of:

- a consent form that is distributed to students; or
- an email sent by the student to the co-ordinator giving their permission to broadcast their email address to other students.

Email addresses of staff and students should only be placed on a publicly accessible website if you have clear written permission to do this. Placing email addresses in "mailto:" fields on a public website will almost certainly result in these addresses being collected and used for sending unsolicited bulk email (spam). There are various techniques which can be used to reduce this problem. Email addresses can be made less machine readable, for example by writing `jsmith(at)nwtafe.edu.au` instead of `jsmith@nwtafe.edu.au`. You should also consider protecting staff members' privacy by using email addresses for roles rather than individuals on websites, for example `enrolments@nwtafe.edu.au` instead of the name of the person currently doing this job.

You should also be careful of email distribution lists. For example, using the 'BCC' field when sending bulk emails will protect the privacy of individual email addresses.

## Making available records of email and chat

There are many circumstances under which one might want to record chat sessions and distribute transcripts of these to other students in the same course, to later students in the same course, or to work colleagues, or to publish or distribute in some way typed discussions that originally took place as part of online learning activities. Many factors will influence whether such actions are a breach of privacy law and it is not possible to generalise. Important considerations are:

- Is the work a 'record' that contains 'personal information' in the context of privacy law? If the author cannot be identified the record will no longer be 'personal information'. This may require more than just removing names as there are many other ways an individual can be identified.
- Is the use part of the primary purpose for which the information was collected, or an allowed and related secondary purpose? Refer to the Federal Privacy Commissioner's *Guidelines to the National Privacy Principles* for more discussion of this point.
- Was consent granted for the collection and use in the way proposed?

## Student enrolment records

Individual student records are clearly personal information and your organisation should already have in place policies that cover aspects such as secure storage and informing students at the time of enrolment how this information will be used. All RTOs are required to provide statistical information as part of the AVETMISS national data collection. However if you have a separate student management system for online delivery you may also want to collect and share this information for research and planning purposes. It is always desirable to inform people of how information will be used at the point of collection. Provided the information is sufficiently de-identified, sharing and publishing statistics of enrolment information is not in itself a breach of privacy law. It is important to note however that simply removing student names, student number etc. may not be sufficient to fully de-identify the information. For example if there is only one male student in a course over the age 30, then anyone who knows that student can ascertain all the other collected data about that person if the de-identified enrolment data is published. Similar issues can arise if numbers are small in statistical breakdowns.

## What you can do to minimise privacy problems

- For any service you are offering, consider whether it is practical for this to be offered anonymously (NPP 8), either as the standard way of providing the service, or as an alternative if desired by a user.
- Consider carefully what personal information you actually need to collect and use. Do not collect information unless there is a clear need for it. It is easy to set up forms and databases to collect information, but in many cases the quality and usefulness of information that is optional or volunteered by users is not very high.
- Be clear why you are collecting information and make sure that the reasons you are collecting the information and what you intend to do with it is made very clear at the point of collection.
- Do not store information which is not needed – for example if your system is set up correctly it is not necessary to store a user's credit card number once a transaction has been approved.

- Remove personally identifying information from databases before the data is transferred to other people for purposes such as evaluation, reporting, and analysis of website usage.

## Developing a privacy policy

In general your organisation should have a *single* privacy policy which sets out *all* the ways you collect, use and manage personal information, including online services, as opposed to having separate policies for particular situations.

If you are responsible for setting up online services you should ensure that your organisation's policy covers all aspects of your online services. Resources listed in the *Useful resources* section of this Guide may assist.

Due to the number of different privacy rules and different functions and tasks carried on by different organisations, it is not possible to provide a definitive list of everything that should go into a privacy policy. Ultimately this is an issue which organisations should seek specific advice on.

However it is possible to list a number of general questions or categories which organisations may need to consider and address in their privacy policy:

- Who is bound by the policy? (for example an organisation may have several subsidiary or related organisations, overseas branches etc.)
- What laws cover the organisation bound by the policy?
- Does the organisation comply with any industry privacy code?
- What kind of personal information does the organisation collect?
- How is the information collected? (for example manually, by email, through the use of automatic collection mechanisms such as web cookies)
- If cookies are used, can the user switch them off?
- How will the organisation use the personal information it collects? (Usage should be specified, including whether there are primary or secondary uses of the information. If information is collected in relation to the user's computer, how will this information be used?)
- To whom may the organisation disclose personal information? Can a person object or prevent this disclosure? If so, how?
- How does the organisation protect personal information? (eg, are any internal policies in place, do computer systems use technologies such as encryption or firewalls?)
- How can a person update their personal information, check what information is held about them or correct any errors?
- How will a person contact the organisation to manage their privacy issues? Does the organisation have a privacy officer?

In developing a privacy policy you might also choose to review the existing policies of similar organisations in the light of your own operations and the requirements of the National Privacy Principles. Examples include:

- The Office of the Federal Privacy Commissioner's own privacy policy is an example of a policy covering use of a website:  
<http://www.privacy.gov.au/policy/index.html>
- The privacy policy for the flexiblelearning.net.au site:  
<http://flexiblelearning.net.au/frameworkstandards/privacy.htm>

- The *AEShareNet* privacy policy provides an example of a policy which covers a range of situations, from anonymous web browsing through to transactions in which a users login is recorded as part of a legal transaction.

<http://www.aesharenet.com.au/siteInformation/legal/116privacy.asp>

Deleted: <http://www.aesharenet.com.au/policy/116privacy.asp>

## Useful resources

### Legal issues in flexible learning website

This website contains useful resources on a range of legal issues: copyright and intellectual property; content regulation; privacy; freedom of information; telecommunications; and e-commerce and trade practices law. It includes:

- An **Information Kit** containing a resource book and four booklets with scenarios relating to legal issues experienced by different VET professionals (practitioners, developers, librarians, managers).
- **Scenarios:** Managers, practitioners, developers and librarians contributed examples of their legal issues and experiences in the area of flexible learning. These issues and experiences were then given to a lawyer to comment on. The lawyer's responses provide general information for each of the scenarios.
- **Legal Questions and Answers:** Between October and December 2002 members of the Vocational Education and Training (VET) sector posed questions relating to legal issues in flexible learning to a legal team from Minter Ellison lawyers. The questions and the lawyers' responses are provided in this section of the website.

Some of the material above on specific situations is taken from the "Legal Questions and Answers" and has been generalised from answers to specific questions. You will find the full questions and detailed answers on this site at:

<http://flexiblelearning.net.au/legal/>

### Guidelines for Federal and ACT Government Websites

These Guidelines were prepared by the Office of the Federal Privacy Commissioner to assist Federal and ACT government agencies to adopt best privacy practice and comply with the Privacy Act in respect to their websites. If personal information may be transmitted, published, solicited and collected via the Internet, agencies need to consider the relevant privacy implications when considering their web strategies.

<http://www.privacy.gov.au/internet/web/index.html>

### Guidelines on Workplace Email, Web Browsing and Privacy

These Guidelines were prepared by the Office of the Federal Privacy Commissioner. Their purpose is to recommend steps that organisations can take to ensure that their staff understand the organisation's position on this issue through the development of clear policies.

<http://www.privacy.gov.au/internet/email/index.html>

### OECD Privacy Statement Generator

The Organisation for Economic Co-operation and Development (OECD) has developed a Privacy Statement Generator primarily as an educational tool to assist organisations within member countries develop privacy statements. You can access

this at:

<http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>

Although not specific to Australian privacy law, the OECD generator will guide you through a series of question and generate a draft privacy statement. This is a particularly useful process if you refer to the Help file at each stage of the questionnaire.

## **Acknowledgement**

This Quick Guide draws heavily on material produced by the *Legal issues in flexible learning* project which contains material produced by Minter Ellison lawyers in response to scenarios and questions produced within the VET sector. Minter Ellison are not responsible for the content of this Quick Guide.

**For more information contact:**

**Framework Communications Team:**

**Phone: (07) 3247 5511**

**Fax: (07) 3237 0419**

**Email: [enquiries@flexiblelearning.net.au](mailto:enquiries@flexiblelearning.net.au)**

**Web: [flexiblelearning.net.au](http://flexiblelearning.net.au)**

**Locked mail bag 527 GPO**

**Brisbane QLD 4001**