

## **CONDUCTING UNIVERSITY BUSINESS ONLINE** **LEGAL ISSUES**

### **Introduction**

At a basic level, electronic commerce means commercial activities including the promotion, marketing, supply, order or delivery of goods and services carried out through electronic networks. In the University context, the concept also needs to include all other internal and external processes and operations which are carried out over electronic networks.

In this paper, we have categorised the University's current and potential online activities according to the people or organisations with which the University deals. The last section deals with general legal and management issues. For each category, we have provided a brief outline of the legal issues which arise and which need to be considered in this new environment.

### **Online activities**

#### **1 Staff**

1.1 Staff involvement with the University's online activities may be divided into the following areas:

- use of the University's computer facilities;
- developing websites; and
- publication of course materials online.

## **1.2 Use of the University's Computer Facilities**

The University's computer facilities under the University's Computer Regulations (Reg. 37.1) are defined to include, amongst other things: the University network; computer equipment; data and software owned or licensed from third parties; and online services hosted or carriage services provided by the University including internet, intranet and email services.

The use of the University's computer facilities by staff members is governed by:

- the Computer Regulations which prescribe rules governing all aspects of access and use of the computer facilities;
- the Code of Conduct which impacts on, amongst other things, the use of University resources and use of confidential information;
- the Internet Code of Practice which imposes restrictions on the use of the University's network to access the Internet and Internet services including electronic email and the World Wide Web. The Internet Code of Practice outlines clearly the parameters for the use of the computer facilities in order to minimise the potential risks for the University. It also serves to remind the users of the power conferred on the University with respect to any unauthorised use of the University's network. Recent cases suggest that employers should regularly inform its members of the restrictions in the online environment/use of email and the employer's ability to monitor and suspend access in some circumstances (Ansett's case);
- privacy laws and any privacy policies of the University which clearly state the extent to which personal information of staff and students may be used by staff members.

## **1.3 Developing websites**

Where staff members are involved in the development of websites for University purposes the following matters need to be addressed:

- ownership of intellectual property in the elements of the website such as the design, software, tradenames, photographs, film and text. For example, when a web designer is engaged as an independent contractor, it is essential that a formal agreement is entered into to address issues such as intellectual property ownership and the right of the University to make modifications to the web site without the permission of the web designer.
- third party rights and use of third party material;
- a consistent approach in the presentation of the style ("look and feel"), quality control and currency of information.;

#### 1.4 **Publication of course materials online**

In addition to other matters described in this section, when the computer facilities are used for online teaching and for the publication of course materials, copyright issues in the reproduction and communication of third party materials must be addressed.

## 2 **Students**

### 2.1 The University's electronic relationship with students can be separated into three areas:

- passive provision of information or “electronic brochures”;
- provision of learning materials; and
- other interactive transactions.

### 2.2 “**Electronic brochures**” include course listings; handbooks; information about scholarships, grants and fees; library catalogues; printable forms; and other basic information services. Legal issues arising from the provision of these services include:

- ensuring advertising and marketing information is clear and accurate, as it will be widely available to the public (consumer protection laws). Web site designers should not assume that people will access all links – so all relevant information needs to be included in a highly visible way;
- ensuring outdated information is removed from web sites (consumer protection laws);
- archiving material which has appeared on web sites (evidence);
- accessibility – web sites need to be constructed to allow screen-reading and other software to have the best chance of interpreting their contents. Information should be made available in alternative formats as required (discrimination and equal opportunity laws).

### 2.3 **Electronic learning materials** could be in passive or interactive formats. The legal issues set out in 2.2 will also apply to electronic learning materials. Further legal issues include:

- management of third party or other licensed materials which are made available to students online (contract/copyright);
- the prohibition under the Higher Education Funding Act on charging fees (section 18(1)(d)). If the University directly or indirectly requires students to pay money, for example if it adopts a “user-pays” regime in computer labs, then it needs to determine whether these charges could be interpreted as being prohibited “tuition fees” under sections 3 and 18 of the Act.

2.4 **Other interactive transactions** between the University and students include enrolment and online payment services. Legal issues, in addition to most of those described above, include:

- adherence to codes of practice and conduct, for example the Electronic Funds Transfer Code of Practice. The second draft of the expanded EFT Code of Practice is available on the Australian Securities and Investment Commission web site at [www.asic.gov.au](http://www.asic.gov.au). The Code of Practice covers many relevant issues such as authentication, security, availability of terms and conditions, record-keeping, liability for unauthorised transactions, rights and obligations under stored value systems (Smart Cards), and privacy.

### **3 Suppliers**

3.1 The Electronic Transactions Act (Victoria) 2000, which came into effect on 1 September 2000, confirms that electronic contracts are as valid as “written” ones.

3.2 The University needs to consider how traditional commercial principles will apply to online dealings with suppliers. The basic issues underlying the successful formation and completion of contracts are that the parties know:

*who they are dealing with;*  
*where the other party is based;*  
*whether financial consideration can be validated; and*  
*which jurisdiction controls the contract.*

3.3 The University’s procurement policies and procedures need to clearly apply to electronic contracts as well as paper-based contracts. The same or equivalent safeguards need to be built into University systems – for example, the requirement for approvals and for contracts to be signed by an authorised University signatory needs to be maintained. Similarly, where the University requires an authorised signature from another party, an acceptable digital alternative needs to be specified.

3.4 Standard contract terms, including references to jurisdiction, receipt of electronic communications and other issues, need to be applied in the e-commerce environment just as they are applied to paper based transactions.

## **4 Legal/Management Issues**

### **4.1 Archiving/record-keeping**

Current record-keeping requirements need to be maintained. For example, many University records are covered by the Public Records Act 1973. Other specific pieces of legislation and standards also need to be considered such as the GST Act which requires that evidence of transactions, including tax invoices, be kept for 5 years and the Standard for the Management of Electronic Records established under the Public Records Act.

### **4.2 Access and authentication**

Currently, the Telecommunications Act allows the University to provide internet access, without having to obtain a licence, to a restricted group of users. These restrictions are mirrored and extended by the University's agreement with AARNET. Not only do these restrictions need to be strictly followed by the University, they also need to be made clear to users through their acceptance of appropriately drafted terms and conditions of use. Authentication systems supporting these legal requirements will play an essential part in ensuring the University's compliance.

### **4.3 Business procedures**

Adherence to standard University business procedures needs to be maintained in this new environment.

### **4.4 Copyright Act - Digital Agenda amendments**

Recent significant amendments to the *Copyright Act 1968*, which came into operation on 4 March 2001, impose new obligations on the University in the online environment. Among other things, the University must ensure that it complies with the new legislative requirements when copyright materials are copied and communicated (by electronic transmission or made available online) to the staff and students of the University for educational purposes. See <http://www.latrobe.edu.au/www/copy/>

### **4.5 Liability of the University as ISP and publisher**

In some circumstances the University will be deemed to be an internet service provider or a publisher (e.g. under the Copyright Act, the Broadcasting Services Amendment (Online Services) Act, the Telecommunications Act, the Classification (Publications, Films and Computer Games) Act) which may expose the University to potential liability.

The University must ensure that it complies with all relevant laws which may involve doing the following:

- developing authorisation/access procedures for content which is to be made available online;
- removing “objectionable material”, as defined in the Classification (Publications, Films and Computer Games) Act, from the network;
- removing “prohibited content” pursuant to a “take-down notice” under the Broadcasting Services Amendment (Online Services) Act;
- restricting access by minors unless the consent of the parent or guardian is obtained;
- removing defamatory material from the network;
- preventing ongoing infringement of intellectual property e.g. the unauthorised reproduction of music or films;
- prohibiting any “framing”, which means to incorporate the content of the other site into the University’ frame so as to pass off the services/content of the other site as the University’s, without the owner’s permission;
- making sure that any “deep linking”, which means bypassing the home/front page of the target site, does not give rise to any liability. Where the linked site is a commercial site which generates revenue from advertisements, it is safer to link to the home/front page or obtain permission for the deep linking;
- in the case of any linking, ensuring that an appropriate disclaimer of liability is inserted on all web pages to avoid legal responsibility for the information contained in the target site.
- complying with relevant industry codes of practice. For example, the University, under the Copyright Act, may be deemed to have authorised infringement of copyright if the University does not comply with relevant industry codes of practice.

#### **4.6 Updating**

Processes should be in place to ensure that information available on the University’s website is clear, accurate and up-to-date and that old sites and information are removed regularly. It is in the University’s interests to have some sort of archive of material which has appeared on web sites. The archive need not be in electronic form.

#### **4.7 Domain names**

- Registration of domain names on behalf of the University should be approved by the University Secretary.
- The University should reserve names of different country domains where the University has a presence or a potential presence.
- The University may have to consider registration of trade marks in order to obtain some protection against domain registration by external persons (cybersquatters).

#### 4.8 Risk Management

As part of the University's risk management it should do the following:

- require users, on the grant of a computer account, to acknowledge that they have read and understood the rules governing use of the Computer Facilities and agree to comply with them. The agreement entered into by the University, Optus and AARNET Pty Ltd requires the users to grant an indemnity;
- ensure that users are regularly made aware of the University's statutes and regulations and policies governing the use of the Computer Facilities. This may be done by articles in the University's publications and by periodically requiring the users to click when they log on to the network an acceptance of the conditions for use of the Computer Facilities;
- from time to time have appropriate warnings on the screen when users log on to remind users of what is prohibited under the Internet Code of Practice and the Computer Regulations;
- ensure that the University is adequately insured for its potential liability in the online environment.

#### **Note**

The Ministerial exemptions under the Telecommunications Act have been extended until mid 2001. After that date, the provisions of the Telecommunications Act may impose onerous obligations on the University. This situation is currently under review by the University and any important changes will be brought to the attention of relevant personnel within the University.

Should you require any further information on these issues, please do not hesitate to contact the undersigned.

*This article provides general information only. It is not a complete or definitive statement of the law on the subject matter. Formal legal advice should be sought in relation to particular matters.*

31 July 2001

**Gilbert Ducasse**  
Deputy Director, Legal Services

**Hilary Cantwell**  
Solicitor, Legal Services

