

# **Appendix G**

**The University of Bolton Case Study: Part 3**

**Authors: Dr R. J. Hood and Roy Attwood**

**IPR in International e-Learning Programmes  
Case Study from The University of Bolton**

**Part 3. Intellectual Property Protection (IPP)  
- A Practical Approach**

**January 2005**

**Dr. R.J. Hood and Roy Attwood**

The University of Bolton  
Deane Road  
Bolton  
BL3 5AB

## CONTENTS

<b>ABSTRACT</b> .....	1
<b>ACKNOWLEDGEMENTS</b> .....	1
<b>1. LESSONS FROM THE COMMERCIAL WORLD</b> .....	2
1.1 Information processes in e-commerce.....	2
1.2 Commercial example of multiple levels of protection .....	3
1.3 Ease of copying web content.....	3
1.4 Conclusions .....	4
<b>2.0 VALUE OF E-LEARNING COURSEWARE</b> .....	5
2.1 Interested parties .....	5
2.2 Value when IPR is included in the sale.....	5
2.3 Value when IPR is not included in the sale.....	6
2.4 Value to other providers who do not recognise copyright law .....	6
2.5 Value of access for students registered with the legitimate provider.....	7
2.6 Value of access for students not registered with the legitimate provider .....	7
<b>3.0 INTERNATIONAL ELEARNING PROVISION</b> .....	8
<b>4.0 EXAMPLE OF A PRACTICAL APPROACH TO PROTECTING IP</b> .....	9
4.1 E-learning example of multiple levels of protection.....	9
4.2 Focus on added value .....	10
4.3 The "thin client" approach to restricting access to licensed software .....	10
<b>5.0 A GENERALISED PRACTICAL APPROACH TO PROTECTION</b> .....	12
5.1 Web site .....	12
5.2 Remote access facility.....	12
<b>6.0 FURTHER WORK</b> .....	13
<b>7.0 CONCLUSIONS</b> .....	13
<b>8.0 REFERENCES</b> .....	14

## APPENDIX

1. A thin client approach to protecting teaching material

## **ABSTRACT**

This part of the report considers the issues associated with attempting to protect the intellectual property residing in courseware developed for an international e-learning programme. It begins by examining how successful the commercial world has been in transferring information securely over the internet and in protecting intellectual property rights. A discussion follows on the value of e-learning courseware and the effect of going international. Given the experience of the international commercial sites, some conclusions are reached.

The approach taken at Bolton is put forward as an example of a practical and rational response to the findings described up to this point.

Finally an attempt is made at defining a generalised practical approach to protection where both web content and a thin client facility are involved.

## **ACKNOWLEDGEMENTS**

Many people have contributed to the developments described in this report, notably Jeff Ormerod, Phil Knowles, Ian Charlson, Mark Williamson, Roger Kirkman, Neil Cole, Matt Brocklehurst, John Cross, Matt Lloyd, Dan Rowles, Martin Jones, Gary Burns, Mark Power, Paul Sharples, Angela Tinwell and Chris Frost. The authors would also like to thank Dr Neil Ringan of eLaB at The University of Bolton for proof reading the report and making numerous other suggestions for improvement.

## **1. LESSONS FROM THE COMMERCIAL WORLD**

### **1.1 Information processes in e-commerce**

International e-learning programmes typically involve transmitting information in electronic form over the internet, with apparent associated risks of interception, illegal copying and exploitation by one or more third parties. Commercial companies have been grappling with the very same issues for many years so it is instructive to examine the successful business models that have emerged and the extent to which they rely on technology and legal systems. Four separate processes involving information can be identified:

#### **Customer authentication**

There must be confidence that the person requesting information or using the service is who they say they are and is not impersonating somebody else. Authentication using a smart card or a signing in procedure (with encryption), have worked reasonably well. New developments in biometrics such as finger print, facial, voice or iris recognition will bring further improvements where the cost of additional hardware can be justified.

#### **Secure transmission**

The information passing in one direction or the other should not be leaked en route. i.e. it should not be possible to intercept and copy the transmission. The internet is not a secure carrier but it can be made secure by encrypting the data stream or by adding levels of security. Establishing an encrypted virtual private network (VPN) connection achieves commercial levels of security.

#### **Copy protection**

This issue only arises where the transaction has resulted in "content" being passed to the customer in electronic form. Normally the customer will have entered an agreement not to pass on the content so there is likely to be recourse to law if the customer breaks the agreement.

The entertainment industry has campaigned for technical safeguards against copying every time a new media format is developed. Despite its commercial might, it claims still to be losing large sums from piracy and periodically takes the legal route with heavily publicised legal actions for damages against a very small sample of law breakers. The industry is aware that the legal route does not offer a full solution and invites a backlash of public opinion, so uses it sparingly.

The record industry is now trying a different approach and is receiving a large number of small payments for downloading individual songs. Downloaded material is traceable through digital codes which may be used to inhibit further copying.

#### **Promotion by largesse**

All successful e-commerce companies have developed some means of providing value before a purchase takes place. Virtually all sites are generous in the amount of information provided free of charge. In the area of software, some companies offer free use of their products for a trial period; others give away a cut-down version of the product (crippled software), while others give away the product and invite donations (freeware). The purpose of this largesse is to provide an incentive to visit and re-visit a site, and to tell other people to do so. Success brings further success as search engines give the site more prominence. In many cases sites can be personalised, all aiming to build customer loyalty and ease the decision to make a purchase.

## 1.2 Commercial example of multiple levels of protection

Consider a website for online banking. Anyone can read the bank's home page; indeed the bank goes to some lengths to encourage them to do so because the page is a form of advertising. To gain access to their personal accounts customers move to a different server and a secure link is established by passing certificates. Data in both directions is then encrypted so details such as the account details and the password are not transmitted in plain text.

When a user has gained access to their account details they may view or print the information. However, some transactions are further protected and require additional user verification before they are sanctioned, such as paying a bill electronically. As a further security measure, to ensure that an account is not left open accidentally, access is terminated automatically after a period of inactivity.

In the above example the bank's web site serves the dual purpose of marketing and day-to-day business. Despite the fact that the home page is open to everyone, clients have confidence that their account will remain secure. The bank is using technology to restrict access to what is perceived to be valuable. If we were to go into this more deeply and include the arrangements for access by the bank's employees, we would find there are many different levels of access and protection at work.

## 1.3 Ease of copying web content

Anything that can be read on a screen can be copied electronically if the recipient so chooses. Many techniques exist for making copying more difficult but they can all be overcome if there is sufficient incentive. For those with enough patience it will always be possible to "capture" repeated images of the screen and then pass the images through character recognition software.

Software is readily available for taking an electronic copy of all the pages and images within a particular site (e.g. "Web Grabber"). These pages can then be re-hosted and served illegally.

### **Key Point 1**

There is no protection against the unscrupulous. The internet does not recognise national borders so it will always be possible for somebody to gain access legitimately and then move to a country that does not recognise copyright law and download and re-use everything available. However, they will only do this if there is a sufficient incentive.

## 1.4 Conclusions

The business processes of E-commerce are still evolving but are sufficiently mature that millions of secure financial transactions take place over the internet daily. Customers and suppliers worldwide have a high level of confidence in the protection afforded by the technical approach taken to security. Legal protection exists but, compared to the volume of transactions, it is very rarely invoked.

### **Key Point 2**

Technologies for protecting electronic content internationally are successful but only up to the point where it becomes financially worthwhile to overcome them. Recognising this, commercial suppliers are developing new ways of doing business on the internet, splitting content into smaller pieces (e.g. songs instead of albums) and devising ways of managing smaller elements (e.g. digital rights management). At the same time they are seeking other ways of adding value (e.g. free home delivery).

### **Key Point 3**

For marketing reasons e-commerce sites provide a significant amount of content free of charge. Access arrangements are then tiered, with higher levels of protection accorded to higher value information.

There are significant differences between e-learning and e-commerce, notably motivation and the added value that an accredited qualification bestows. Nevertheless, the conclusions from the commercial experience may help avoid costly mistakes in attempting to organise an international e-learning programme.

## **2. VALUE OF E-LEARNING COURSEWARE**

### **2.1 Interested parties**

Just as "beauty is in the eye of the beholder", so value depends on the circumstances of the potential buyer. Where e-learning courseware is concerned, the interested parties can be categorised into providers, beneficiaries and contributors.

#### **Providers**

- the owner of the IP (normally the educational institution that has commissioned the work)
- other education providers interested in entering a partnership or franchise agreement
- other education providers who ignore copyright (illegal competitors)

#### **Beneficiaries**

- existing enrolled students
- potential future students who are willing to pay
- potential future students who are unwilling to pay a fee

#### **Contributors**

- authors having moral rights to the IP
- owners of copyright material used within the courseware by agreement

Valuations that might be considered are listed in the following cases and enlarged upon in the sections that follow.

Case 1. Value of courseware sold with full IP rights but safeguards for existing students.

Case 2. Value of courseware sold with a licence for specified use (partnership or franchise).

Case 3. Value to other providers (competitors) who do not recognise copyright law.

Case 4. Value of access by students registered with the legitimate provider.

Case 5. Value of access by student not registered with the legitimate provider.

### **2.2 Case 1. Value when IPR is included in the sale**

E-learning courseware is expensive to develop and has a limited life because the subject develops, syllabuses change and the presentation mechanisms used on the internet themselves change. Furthermore, ownership of the IP brings with it a continual maintenance cost that must be afforded if the courseware is to maintain its value.

High quality e-learning courseware is a necessary prerequisite for a provider to gain a good reputation and build a sustainable business. It has a high value to the institution owning the intellectual property rights because they can derive benefits of fee income and potentially additional revenue from licensed usage by other providers. As these benefits are only available to the owner of the IP, the full value can only be realised if the courseware is sold with full rights to the IP. Under these circumstances the value of the sale will depend on the cost of reproducing the material by some other means. If we ignore other factors such as proof of market demand, then providing the work was undertaken efficiently in the first place, the value is likely to be similar to the cost of production.

**Key Point 4**

Sale with full rights to IP is the only circumstance when a valuation approaches anything like the cost of production i.e. the value is equivalent to the replacement cost.

In all other cases the value of e-learning courseware will be far less and will bear no relationship to the cost of production. This is an important point which is easily overlooked.

**2.3 Case 2. Value when IPR is not included in the sale**

The value of e-learning courseware without rights to IP and without other value added elements (remote access to software, tutor support, or the potential to gain a qualification) is low. As with any other commodity, it depends on supply and demand. If the subject matter is covered in books or elsewhere on the internet, then the value is set by the cost of those alternatives.

If the topic covers very recent developments or it contains particularly instructive images, simulations, animations or access to specialist software, the value will be correspondingly higher.

**Key Point 5**

The value of e-learning courseware to another provider is determined by the potential fee income from using the courseware. However, the fee income is related to the total added value as perceived by the students; courseware may only play a small a part in this.

An e-learning includes several aspects that add value in addition to the courseware. Refer to section 4.2 for an example.

**2.4 Case 3. Value to other providers who do not recognise copyright law**

The value is set by the lowest fee that will allow the competitor to enrol as a bogus student and defeat any protection mechanisms employed.

## 2.5 Case 4. Value of access for students registered with the legitimate provider

Legitimate benefit from the whole package and not just access to the courseware. For this they are prepared to pay the course fee. The courseware cannot be valued outside the context of the whole package.

### **Key Point 6**

The cost of developing e-learning courseware is irrelevant under normal circumstances and should not influence fees charged for accessing the material. The market determines the level of fees which will depend on the total added value of which courseware is only a small part. Refer to section 4.2 for examples of added value.

## 2.6 Case 5. Value of access for students not registered with the legitimate provider

The value to illegitimate students is, in reality, zero because they will be able to find virtually equivalent material on the internet free of charge.

### **Key Point 7**

Attempting to sell e-learning courseware on its own carries a high commercial risk. HEIs that have tried it have been very disappointed and have not recovered their costs. However, some commercial providers have succeeded in making a business this way.

### 3.0 INTERNATIONAL E-LEARNING ENVIRONMENT

Where e-learning provision is somehow constrained within national boundaries, illegal copying for exploitation (i.e. setting up in competition) is not a serious problem. If it occurs within the same country it is likely to be detected and legal action, or the threat of legal action, is likely to be sufficient deterrent. Illegal copying and re-use in another country may well take place but it does not matter and is not worth time and effort in detection or deterrent. As long as customers in the host country are compelled to sign up to the legitimate provider, what happens elsewhere does not affect the revenue stream, so is more of an irritation than a serious threat.

When an e-learning provider chooses to target the international market, foreign competition based on copied resources could be very damaging while at the same time the cost of legal action to defend rights is likely to be prohibitively expensive.

Such competition could result in:

- a reduction of income from students who would otherwise have enrolled and paid a fee
- a reduction of income from other providers who would potentially have paid for a franchise arrangement
- inappropriate or out-of-date courseware remaining in circulation while still bearing the name of the authors and the originating institution.

The difficulty is, as we have seen in section 1, it is impractical to defend internet-based resources against copying where there is a commercial incentive. A more practical approach is to reduce the commercial incentive to copy and at the same time differentiate the product by other means that are more difficult (i.e. expensive) to replicate.

#### **Key Point 8**

E-learning providers targeting the international market should consider seriously how to reduce the commercial incentive to copy, e.g. by making some or all of the courseware available free. At the same time they should identify aspects that add value and are more difficult to copy, and establish a reasonably secure mechanism for restricting access.

#### 4.0 EXAMPLE OF A PRACTICAL APPROACH TO PROTECTING IP IN AN INTERNATIONAL E-LEARNING PROGRAMME

This example refers to The University of Bolton's Postgraduate Programmes in Microelectronics. The website is [www.ami.ac.uk](http://www.ami.ac.uk)

##### 4.1 E-learning example of multiple levels of protection

A simplified site structure is shown in Fig. 1. The main teaching site home page site is open to anyone. General information, such as course details and module specifications, can be freely referenced and printed. The courseware for the first three units in each module is also open to everyone. We perceive this to be an effective marketing device; as it helps prospective students to decide which programme to study. It also helps to ensure they understand the implications of study over the internet before making an informed choice. Employers and sponsors can also see the site and are therefore in a position to take part and help in the decision.

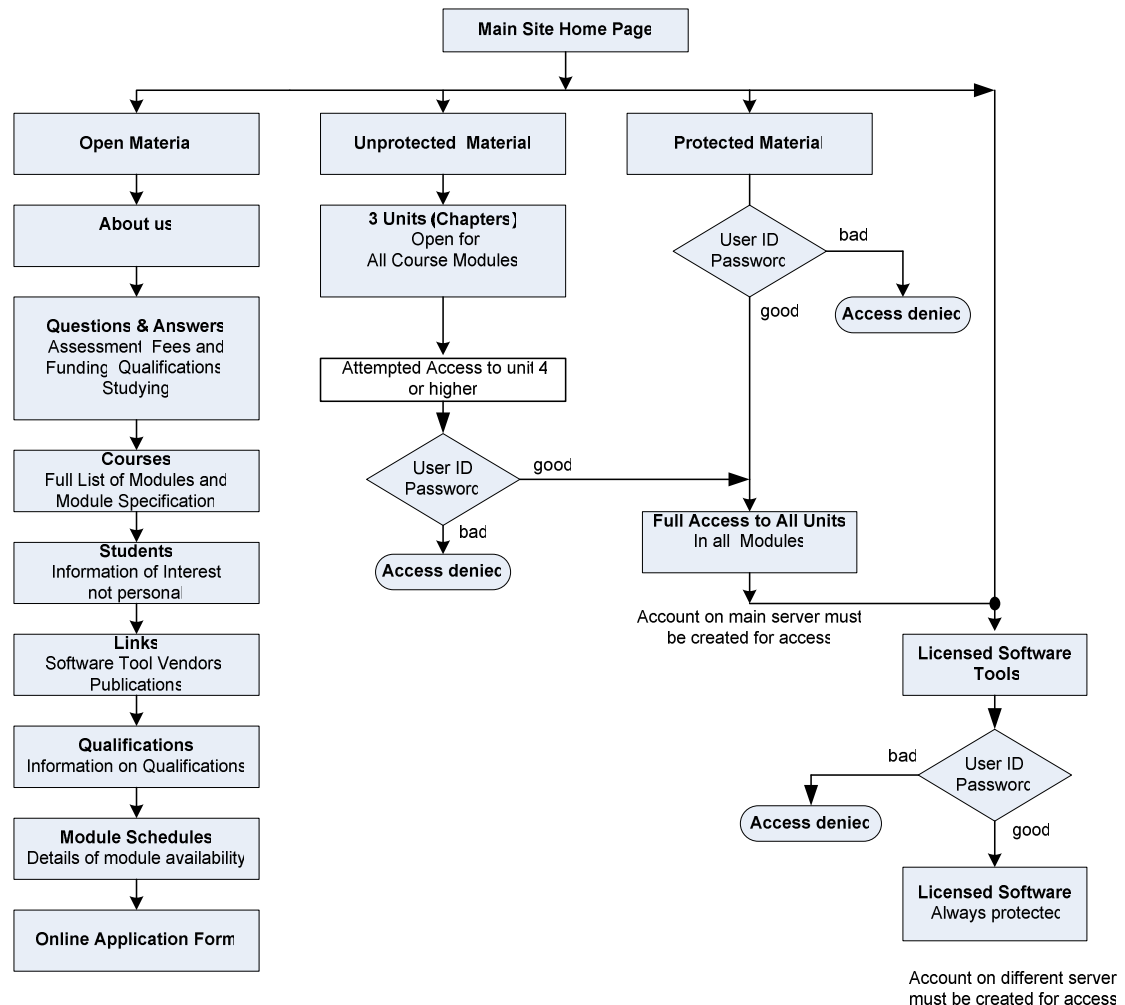


Fig. 1 Example of a practical approach to IP protection

Note that although many different servers are used, the user authentication and serving of application licences is centralised.

When students enrol on a module, an account is set up which allows them to access all the teaching material. Students studying modules involving remote access to licensed industrial software are given additional privileges allowing their account to access the servers hosting the software. The communications tools (email distribution lists, etc) are restricted to the students enrolled on a particular module, together with the tutor.

Thus there are four levels of protection employed:

- open access to the website
- restricted access to parts of the website
- remote access to CAD tools
- protected access to communications tools

Note the similarity of this approach to the commercial example described in section 1.2

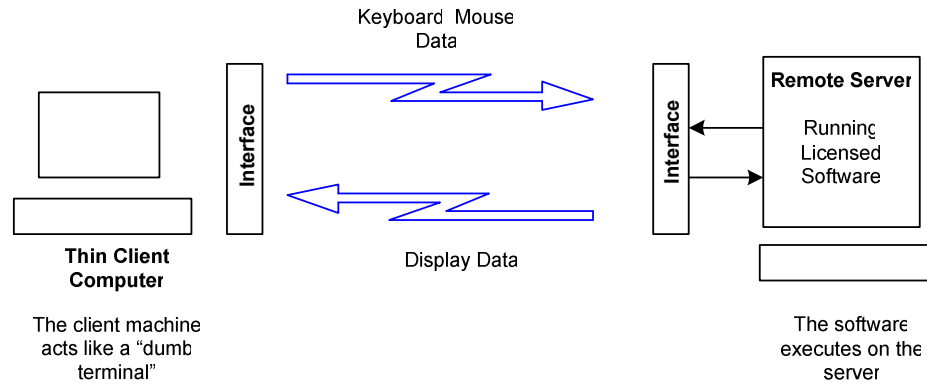
#### **4.2 Focus on added value**

People who enrol on one or more modules of the online postgraduate electronics programmes from Bolton receive the following benefits:

- remote access to state of the art industrial standard software for microelectronics design
- tutor support, guidance and feedback
- access to the courseware for all the modules (not just those they register to study)
- successfully completing a module gains credits towards a postgraduate qualification from Bolton (or elsewhere by credit transfer).
- successfully completing a programme of study leads to an internationally recognised postgraduate qualification.
- access to the central learning support facilities and (through an "Athens" account) to a wealth of online journals and e-books.
- opportunities to borrow books from local universities under the "UK Libraries Plus" scheme (applies only to students based in the UK).

#### **4.3 The "thin client" approach to restricting access to licensed software**

Protection of licensed software using a thin client approach is illustrated in Fig. 2. The licensed software runs on the remote server and the student's computer acts like a dumb terminal. Key strokes and mouse clicks are sent over the internet to the server at Bolton. The interface processes the information at the server and relays it to the application software running on the server. The software behaves as though the commands had been issued on the server. Any visual output from the software is processed by the server interface and sent to the client. The client interface processes the data and sends it to the client display.



**Fig. 2 Illustrating thin client architecture**

Data streams between the client and server are encrypted. Protection is "server side", which means that, access can be controlled to a fine level of detail, for example by type (file type), individual user, user groups, or transaction type (read only, download to client, etc.).

Usage can be monitored from the log files to deter abuse of the educational licenses.

## 5. A GENERALISED PRACTICAL APPROACH TO PROTECTION

### 5.1 Web site

Following this strategy will ensure that the most appropriate things are protected while avoiding protecting things that need not be protected.

**Add value** that cannot be easily copied or duplicated

Consider using a **thin client** approach for **valuable material or resources**

Structure the website to facilitate **marketing**

Structure course material for the **benefit of students**

Structure delivery for the **benefit of students**

Ensure a high level of **authentic student activity**

**Protect what is valuable**, ensuring that legitimate site users are not inconvenienced

Give **open access to as much information as possible**, commensurate with the requirements to protect valuable material

Consider **web site design, administration and maintenance** when specifying the site and during site development.

**Ownership** of material that will appear online should be clearly defined.

### 5.2 Remote access facility

Define the groups who will use the remote access facility. Typically they will include academic authors, site developers, academic tutors, prospective students, prospective corporate clients, students, external examiners, members of validating bodies, etc.

Define the permissions for each group, probably with the use of tables so that all the people involved in the site development can clearly understand the protection strategy.

Very importantly, test protection measurements as the site is being developed.

Protection should be considered as an integral part of e-learning and distance learning course development.

## 6. FURTHER WORK

During the course of writing this report it was suggested that the thin client approach, which has proven a successful means of protecting application software, could provide an effective means of protecting e-learning courseware. The web browser would need to be hosted centrally rather than on the client's machine and detailed control of downloads and printing would then be possible. The arrangement is described further in Appendix 1.

The technical feasibility of the approach has been proven by a few short tests but further work is required to make it easier for the customer to implement and to find ways of overcoming any shortcomings.

## 7. CONCLUSIONS

In this part of the report we have consider practical methods of protecting intellectual property rather than those based on a legal approach.

Valuation of e-learning courseware is a complex matter because the value depends on many factors, including

- the nature of the interested party
- whether or not intellectual rights are included in the sale
- whether or not the stakeholder recognises copyright law
- what other value added items are attached

The University of Bolton has adopted a practical approach to the protection of courseware on an international e-learning programme for the following reasons:

- If teaching material is copied and used without permission it does not incur a direct financial penalty.
- The potentially high cost of litigation, especially in an international sphere, rules out such an approach
- The technical difficulty of imposing effective protection for internet based teaching material
- The value associated with other aspects of the courses (such as the award of internationally qualifications, online tutoring and access to industrial standard software) outweighs the value of the material that can be copied.
- An open access approach facilitates marketing and provides an integrated learning environment for both students and staff.
- Licensed software can be protected effectively by using a "thin client" approach.
- Personal information must be protected in accordance with Data Protection Act

Please refer also to the Key Points 1 - 8 in the text.

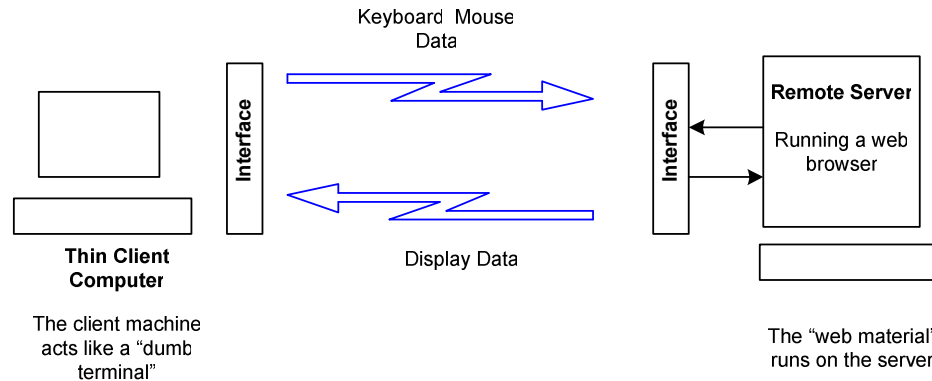
## 8. REFERENCES

- [www.ami.ac.uk](http://www.ami.ac.uk) This is The University of Bolton's site for distance learning MSc qualifications in microelectronics and related subject areas.
- [www.citrix.co.uk](http://www.citrix.co.uk) This is the supplier of the interface software (MetaFrame) used to establish the thin client architecture
- [www.esteem.co.uk](http://www.esteem.co.uk) This is the educational vendor site for the interface software (Citrix MetaFrame) used to establish the thin client architecture.

## APPENDIX 1

### A Thin Client Approach to Protecting Teaching Material

Thin client architecture offers a means of protecting courseware and a strong deterrent to copying. Each user would be constrained to access pages via a browser program running on the server, instead of on the user's PC, as illustrated below. The information transferred to the user (the client) would then be a series of screen images after they had been assembled by the browser program, rather than the data used to construct each page.



#### Protection of teaching material using a thin client architecture

Transactions between the server and client would be under the control of the server administrator, so direct downloads to the client could be stopped if necessary. This arrangement would allow permissions to be controlled to a fine level of detail, even down to individuals and individual pages.

Note that even this approach would not stop somebody who was determined to copy the material - it just makes the job more difficult and therefore raises the necessary level of return required to make it worthwhile. It would still be possible to store a sequence of screen dumps, recover the text and images screen by screen and assemble them into usable web pages again, but the work involved would deter the majority.

The main disadvantages of applying this approach to the protection of teaching might turn out to be:

- the amount of printing allowed would have to be severely curtailed since if users were allowed to print everything (as many like to do), the protection would be breached.
- interface software and sufficient concurrent user licences would need to be purchased for the server. (Interface software for the client is available free of charge).
- the added load on the server might cause some installations to serve pages noticeably slower or reach the point where additional investment in hardware became necessary.
- there would inevitably be additional duties for the server administrator and IT team.
- some animations might run slowly, depending on their complexity and the bandwidth available
- multimedia material, such as video and audio would need to be evaluated over a representative link prior to material release, again because of the bandwidth limitation.