



INSIDE THIS ISSUE

E-Learning Environments Page 1

Virtual Software Page 3

Will you be sunk by student pirates? Page 4

E-LEARNING ENVIRONMENTS GET A SECOND LIFE

Gartner research predicts that by 2011, 80% of web users will be regularly visiting online virtual worlds - and the time people are spending there is increasing. Real world companies looking to make money from this trend have already started opening and making money from in-world offices and showrooms.

The level of participation in Second Life (a 3D virtual world with over 15 million inhabitants) by colleges and universities suggests a growing body of academics recognise the potential such environments have as Virtual Learning Environments (VLE). But what are the educational benefits of these worlds and what are the legal risks to the HE and FE institutions that use them?

E-learning is nothing new to HE and FE institutions in the UK. A study in 2005 showed that 95% of UK universities had some form of VLE and many universities were already using software such as Blackboard, Moodle and WebCT for providing web-based course tools.

Whilst they won't replace off-line education or current e-learning tools, virtual worlds have the potential to support current FE and HE e-learning in new ways, using 3D spaces as new learning environments, for the evaluation of academic performance and to access resources.

3D virtual worlds support a whole host of social interactions. Some universities have created virtual campuses which recreate real world campus buildings and use different media (streamed video and audio, e-mail and chat) and real time interaction to provide live virtual seminars, streamed lectures and virtual classrooms.

The immersive nature of the online environment can help enrich the way students learn and increase learner empowerment. Learners can be virtual tourists visiting museums in other countries (where whole collections are made available to view in an interactive user space which mirrors an actual museum) or can meet with mentors and subject experts from around the world in a virtual lecture hall or even conduct experiments in virtual space not possible in real life.

Specialised learning scenarios within a virtual world allow educators to make more effective use of scarce staff time. Problem solving scenarios have become popular, as the virtual environment allows "lifelike" and real-time role play training. Virtual operating theatres and healthcare courses mirroring real world theatres and wards lead to less anxiety in learners when they ultimately meet with real world experiences. Real life emergency response training sessions run by Stanford University used to need the

whole University campus to be shut. Now the whole scenario is recreated in a virtual world.

There is little doubt that the use of virtual worlds as an online learning resource offers great opportunities to meet the changing needs of students and their interaction with digital resources at both undergraduate and postgraduate level. But institutions who want to make the most of these new learning environments will need to take care to ensure that their staff and students are aware of the key legal risks.

The legal risks of VLEs

When investigating a university in the UK earlier this year the CLA (Copyright Licensing Agency) found that 70% of the materials in one segment of their WebCT environment were infringing copyright. Both students and lecturers had been posting content, articles and links in breach of third party licences.

HE and FE institutions are legally responsible for the content they publish online. The use of new e-learning environments such as Second Life and other web-based applications that allow sharing of documents and files exposes institutions to additional liability. Institutions should revisit and ensure there is a unified policy on the use by

students and lecturers of online resources.

Issues which should be taken into account as part of developing an e-learning or VLE resource include:

III Intellectual Property (IP) & Copyright

Exercising control over what staff and students publish online is difficult. Indeed, the more control that an HE or FE institution operates over an e-learning environment (such as through editorial control) the more legally responsible they will be for illegal, defamatory or infringing content.

Where students and staff are contributing to an online e-learning environment they should be made aware of the risks of posting or uploading materials developed by others. Some, but not all institutions have robust IP and online policies, yet students and staff often believe that if content (especially educational content) is made available online it is free to use.

Students and staff need to understand the importance of obtaining consent before submitting third party content to shared resources - the institution may be responsible for secondary copyright infringement if students or staff post third party material without permission. This could harm the institution's reputation.

Practically speaking, the best way to limit liability is to continue to raise awareness amongst your staff and students of the risks of using third party content in an e-learning environment and operate a fast-track take-down policy when you are alerted to infringing content.

The most important issue for an institution is knowing that it owns or has a licence to the IP in its e-learning materials. It is important that an institution updates and reviews its internal policies and procedures (especially its IP policy), staff, student and developer contracts to ensure that it has the right to re-use work created in a VLE and can easily establish where that work came from.

III Data Protection & security

Most things that students do in a VLE will generate personal data. When students enrol they should sign up to a data protection statement telling them how their data will be used. Institutions should ensure that this statement covers all academic and ancillary purposes the data may be used for, and if an e-learning system is used, any processing on that system, such as for evaluation purposes.

The information collected about a student in an e-learning environment is extensive, from how many times they did a test to when they edited a wiki or submitted an assignment to their tutor. It could also list academic results and submitted work. As a "data controller" (as defined under the Data Protection Act) the institution is responsible for ensuring that data is held securely. This is especially important if the VLE provider offers managed hosting services (like WebCT) and acts as a "data processor". If so, the institution must have a written contract with the provider covering the processing of student data.

III Liability for content posted in discussion groups

Online tutorials, seminars or lectures are largely monitored by teaching staff. If the institution maintains control over what is published the institution is likely to be considered a publisher, editor or author for defamation purposes. This would be true

even for a small seminar group with only two students where a defamatory comment was posted - the closed nature of a tutorial group makes no difference (although the ease with which a student can be identified should act as a deterrent!).

Whilst monitoring of every message is not required, institutions should have a usage policy warning users they will face disciplinary action if they post inappropriate messages and that the institution reserves the right to remove such material. This allows institutions to remove content swiftly and minimise potential damage - it also gives a form of defence to the institution for certain claims surrounding inappropriate content.

We would strongly recommend that all institutions establish clear and robust policies to clarify what is acceptable use by students and staff of e-learning resources - and to allow the institution to act quickly in response to complaints. Institutions should also be aware of their responsibilities to students in e-learning environments, especially their obligations under the Data Protection Act and discrimination legislation. If these issues are not addressed, an institution could expose itself to unnecessary risks which could be damaging to reputation, as well as to finances.

For more information and advice on the application of these topics, please contact:

Des Burley, Partner

T: 0870 763 1107

**E: des.burley@martineau-uk.com or
Robert Coble, Assistant Solicitor**

T: 0870 763 1375

E: robert.coble@martineau-uk.com

VIRTUAL SOFTWARE: THE LICENCE TERMINATOR?

Innovations in software delivery - such as "Software as a Service" (SaaS), open source software (OSS) and virtualisation provide opportunities for HE and FE institutions to increase efficiency and reduce energy costs. SaaS and virtualisation (like cloud computing), in particular, enable greater user flexibility with students and staff able to log on wherever they happen to be, through virtual servers and desktops in a centrally managed environment.

The licensing models used in SaaS, OSS and virtualisation differ from standard software licensing models, and your institution's Software Asset Management (SAM) strategy will often become more complex and burdensome if these software environments are adopted.

Virtualisation has particular concerns. A key benefit is that it saves resources - essentially, redundant or rarely used memory or processing capacity is shared between users. A famous example was the SETI project which allowed PC users across the world to download a screensaver which would analyse radio waves in the search for intelligent life in space. Desktop virtualisation (for example using Citrix, VMware or NetApps) can have additional benefits: PC environments can be standardised (for example, using a single template student desktop); IT maintenance is quicker, the costs can be lower - and it can be carried out remotely; migration to new systems can be simplified; and de-bugging

can be done on a virtual machine with minimal service disruption. This model has a huge impact on SAM.



From a licensing perspective, unless these innovative models are allowed for in licensing agreements, institutions may be in breach of existing software licence agreements for operating systems and application software - which will restrict use - even to the extent that virtualisation may be expressly prohibited.

Care should be taken in rolling out application software to ensure the correct licensing has been obtained. For example, if an application is put on the virtual desktop template and is then accessed across the university or college, then this may require thousands of users to be licensed.

Another concern is warranty cover. Most software vendors provide support only if their software is being used in a standard environment prescribed by them - if problems are caused through use in a virtual

environment the warranty may not apply. Again, unless warranty and licence arrangements allow for virtualisation, applications used in your virtual templates may be unsupported.

More vendors are developing licences that account for software being made available on virtual servers. Typical licence models allow use of applications on a per computer basis (one virtual machine) or on a fixed or unlimited number of virtual machines (per physical machine or at one location) or across the institution (enterprise wide).

Despite these new licensing models, virtualisation will still create a minefield of new issues for software users. Since creating a virtual machine, or deleting it, can take a matter of moments, tracking software use (and tying that up with licences) in virtual environments will make SAM for education institutions difficult.

The Federation Against Software Theft (FAST) is paying close attention to the impact of virtualisation on legal compliance. To ensure you are not breaching your software agreements we recommend that when you consider virtualisation you think carefully about the impact it will have on your software licenses. When negotiating contracts with vendors, you should closely identify what you are getting and how, paying close attention to issues such as warranties and the impact of virtual installation.

WILL YOU BE SUNK BY STUDENT PIRATES?

A survey by the Oxford Internet Institute in 2007 found that students are the "most active users of online entertainment and social networking sites" in the UK. Whilst most students may use their internet access for legitimate purposes, many use campus networks to run peer-to-peer file sharing applications which allow the illegal distribution, copying and storage of copyright materials such as music, films, computer games and other software.

Many HE and FE institutions provide internet access to their students and staff with few restrictions. If your networks are used for illegal file sharing, does this mean that you may be liable for copyright infringement?

The short answer is that you could be liable, but if you operate your internet operations in the right way you may be able to take advantage of some defences available under EU law.

Under the E-Commerce (EC Directive) Regulations 2002 a FE or HE institution offering internet services to staff and students is classed as a service provider and can be held liable for content hosted on its servers. However, as the law currently stands you should only be liable if you have actual knowledge of illegal content on your servers and you fail to remove it.

For several years rights holders and other interested parties have lobbied the government to make service providers

responsible for controlling illegal file sharing on their networks. To date the government has resisted changing the law, with representatives of service providers likening the burden of monitoring all traffic through their networks to asking the Royal Mail to read every letter which passes through their sorting offices.

Whilst it may be the individual doing the copying who faces criminal or civil prosecution for copyright infringement (as has happened to students on college networks in the US) - rather than the service provider who simply hosts the content, it is the institution which would be subject to investigation and associated reputational damage if it is not seen to be acting responsibly.



Although under the E-Commerce Regulations there is no obligation on a service provider to monitor the data on their networks (or to actively seek out illegal activity - unless it is brought to their attention), more and more HE and FE institutions in the UK are developing plans to counter peer-to-peer activity by monitoring their residential and academic networks.

But monitoring your networks could expose your institution to other risks. It will place an additional obligation on you to act quickly to remove potentially infringing content (especially if you are doing more than basic traffic or bandwidth monitoring). If you do choose to monitor your networks (and even if you don't), provided you have a robust notice and takedown policy for complaints and a comprehensive network access policy a court is unlikely to expect you to examine every file on your servers to check if it was legitimately downloaded.

If you would like any further information about this Bulletin, or about our work for further and higher education clients, please contact:

Des Burley, Partner
T: 0870 763 1107
E: des.burley@martineau-uk.com or
Robert Coble, Assistant Solicitor
T: 0870 763 1375
E: robert.coble@martineau-uk.com