

23 November 2007

**Please note:** this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

## Table of Contents

1. Introduction.....	1
2. Liability for Defamation.....	2
Godfrey v Demon.....	2
Innocent Dissemination – the Legislation .....	3
Electronic Commerce (EC Directive) Regulations 2002 .....	4
Actual Knowledge.....	5
Defamation, Liability, and Online Discussion Groups.....	6
3. Terrorism.....	6
4. Responsibility for Obscene Publications .....	7
5. Secondary Copyright Infringement .....	7
Removing Material from Publication - Free Speech.....	8
6. Should an Institution Moderate Content? .....	8
7. Conclusion .....	9
8. Sources .....	10

If you have Adobe Acrobat Reader installed on your computer, you may download a [PDF version here](#). *(Recommended for printing.)* Acrobat Reader is available from [Adobe's web site](#).

## 1. Introduction

Providing computers and internet access to students and staff means that responsibility for what they do online can, in certain circumstances, rest with the institution. This Internet Service Provider (ISP) Liability Overview paper considers the extent to which FE or HE institutions are responsible for content which is made available on their computer systems.

FE and HE institutions are legally responsible for their own published content and they must ensure that it does not infringe the rights of others. In general making materials available on a website, or other electronic forum will be considered publishing where the institution exercises editorial control over the content. Institutions may also be held liable where the actions of employees in the course of their employment cause harm to others (known as vicarious liability). Likewise, where as a result of action or inaction they cause harm to their own users or others, or fail to fulfil duties placed upon them,

they could be held to be negligent. Such liability is likely to arise in the electronic as well as the physical environment.

The legal position is further complicated where an institution acts as an intermediary, for example, as a service provider or as a 'host' of information for others. Usually it will be clear when an institution is publishing its own materials in the traditional sense. However with information which is accessed via, or stored on, an institution's computer network and, with the provision of forums where student and staff users are able to upload their own content, it may be less clear where responsibility for its publication lies.

Can an institution avail of the defences to liability (outlined below) which the more conventional providers of information services benefit from?

## **2. Liability for Defamation**

It has been in the highly confrontational area of defamation law where litigation has determined where legal responsibility lies for the online hosting, publishing and possession of unlawful and illegal content.

Defamation is, essentially, concerned with the publication of lies, or untruths and a defamatory statement is one which lowers the claimant in the estimation of right thinking members of society. The general rule of UK defamation law is that the publisher of a defamation faces liability and this applies to FE and HE institutions as publishers in the same way as to any other publisher. So where an institution maintains control over what its users publish, it is likely to be considered a "publisher" of this material for the purposes of defamation.

Liability for a defamatory statement may also be extended to an institution under the principles of vicarious liability or because, in providing online access facilities, the institution is directly liable as a publisher or disseminator of the offending statement.

If the institution exercises any kind of editorial control over the content of its users then the institution is likely to be classified as an author, editor or publisher and will be potentially liable accordingly if the content is defamatory.

Unfortunately, if the institution decides not to monitor its content or respond to complaints, whilst it is not likely to be classed as a primary publisher it is likely to be treated as not having taken reasonable care in relation to the publication and may therefore be treated as a secondary publisher.

So what responsibility has an institution when an individual publishes a defamatory statement about someone else by means of an institution's computer system and is the institution liable as secondary publisher?

### **Godfrey v Demon**

The potential liability of online service provider's in relation to content which they handle has provoked much debate in the UK since 1999, when the Godfrey v Demon defamation judgment [(1999) QBD, [1999] 4 All ER 342] became the first UK case to find such responsibility on the part of an ISP. This was a preliminary hearing in order to establish whether the ISP could take advantage of the so called 'innocent dissemination' defence in section 1(1) of the Defamation Act 1996.

An unknown person, purporting to be Dr Laurence Godfrey, a lecturer in physics, mathematics and computer science based in London, made a defamatory posting which appeared on Demon's news server in the UK. The posting could be read by Demon's customers. When Mr Godfrey asked Demon to remove the posting (having explained that it was a forgery), Demon did not do so. The court found that up until receiving notification of the existence of the allegedly defamatory posting, Demon could not have had sufficient reason to suspect that it was not made by Mr Godfrey. However, from the point that actual knowledge was received, the defence was no longer available.

### **Innocent Dissemination – the Legislation**

The defence of 'innocent dissemination' of a defamation is available to secondary publishers and intermediaries where:

- they are not the “author, editor, or publisher” of the defamation.
- they did not know and had no reason to believe that the statement in question was defamatory
- they took reasonable care in relation to the publication of the statement in question.

Further, under Section 1(3)(e), of the Defamation Act 1996 an intermediary is not considered to be the “author, editor, or publisher” of a defamatory statement:

“...if [the intermediary] is only involved...as the operator of or provider of access to a communication system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.”

The key thing here is that an ISP (or any other intermediary with no knowledge of the defamatory material complained of) will lose the protection of section 1 if it is given notice of the defamatory material and does not delete that material. As a result, any FE or HE institution should treat a notice of complaint seriously and investigate it immediately.

### **In Summary**

Where there is neither actual knowledge of the defamation nor awareness of any facts or circumstances from which an FE or HE institution could reasonably have been expected to be aware of the defamation, and the institution has taken reasonable care in relation to publication of the statement in question, the defence is likely to be available to the institution. Upon receipt of notice of a claimed defamation, the institution should, of course, remove the posting straight away.

There is a very fine path for FE or HE institutions to tread between the requirements in section 1(1) (taking reasonable care in relation to publication) and the defence in section 1(3) (having no effective control).

On the one hand they must not know of and have no reason to believe that material is defamatory and must take reasonable care in relation to its publication, as well as taking steps to remove offending material on receipt of actual knowledge. On the other hand, by going too far in monitoring their users and their servers, they may fall outside the exemption in section 1(3) and could face liability as a publisher.

## **Electronic Commerce (EC Directive) Regulations 2002**

Since July 2002, the requirements of the Electronic Commerce (EC Directive) Regulations 2002, which give effect to the European Electronic Commerce Directive (known as the e-Commerce Directive) must be considered. The Regulations limit the liability of service providers who unwittingly transmit or store unlawful content provided by others in certain circumstances. There are three categories of service providers whose liability is thus limited by the Regulations; those who transmit information (i.e. 'mere conduits'), those who engage in "caching" information, and those engaged in "hosting" information.

The relevant parts of the Regulations apply to the "service provider" of an "information society service". These terms are defined such that an FE or HE institution offering internet and storage services via its servers to staff and students are included. Institutions should only be liable for prosecution if they have "actual knowledge" of illegal content held on their servers and fail to remove it.

### **Qualified Immunity**

Probably the most significant of these provisions on ISP content liability is Regulation 19, which provides a qualified immunity for ISPs in respect of third party provided material hosted on the ISP's servers. This immunity, which applies in respect of both civil and criminal liability, is subject to the following conditions:

- The service provider has no actual knowledge (see below) of the content in question. Once the service provider is in receipt of actual knowledge of the illegality, it must act to remove or disable access to the material as quickly as possible.
- The service provider is not aware of facts or circumstances from which the illegality of the content in question should have been apparent.
- The user responsible for providing the content in question was not "acting under the authority or the control of the service provider" - an employee of a university putting the information on the server in the course of his employment, for instance.

In most cases, a FE/HE institution staff member or student will not be acting either in the course of his or her job or with the authority of the institution by posting illegal information to the servers - for instance, placing obscene material online, or posting a defamatory message to a bulletin board.

These conditions essentially apply an intermediary liability standard in respect of all third party provided content that is the same as that already exists for defamation under section 1 of the Defamation Act 1996.

Further detailed information on the e-Commerce Directive is available in the document "FE/HE Institutions and Liability for Third Party Provided Content" by Gavin Sutter on the JISC Legal website at - <http://www.jisclegal.ac.uk/publications/thirdpartycontent.htm>.

### Actual Knowledge

With regard to the requirement of 'actual knowledge', the court in a 2006 case, **Bunt v Tilley** and others [2006] EWHC 407, held that: "an ISP which performs no more than a passive role in facilitating postings on the internet cannot be deemed to be a publisher at common law." Therefore, FE and HE institutions may rely on this case to argue that they are not liable if they do nothing more than facilitate publishing in the same way that an ISP would.

However, if the institution is the actual publisher or has been put on notice, then they will have the requisite actual knowledge and are likely to be liable. In the words of the court: "if a person knowingly permits another to communicate information which is defamatory, when there would be an opportunity to prevent the publication, there would seem to be no reason in principle why liability should not accrue."

**Source:** Periodical Publishers Association (PPA) -

[http://www.ppa.co.uk/cgi-bin/go.pl/legal/article.html?uid=10678&topic\\_uid=43](http://www.ppa.co.uk/cgi-bin/go.pl/legal/article.html?uid=10678&topic_uid=43).

**Bunt v Tilley** concerned whether three ISPs could be held liable for alleged defamatory postings made in internet chat rooms by their respective customers (who were also being sued by the claimant) on the basis that the ISPs, as intermediaries, had provided the route for the third parties to make the defamatory postings in the first place. **Bunt v Tilley** was the first time that intermediary defences under the eCommerce Regulations had been considered in detail (Regs 17-19). The defendant ISPs were able to rely on the following:

- AOL and Tiscali relied on the "mere conduit" and caching defences;
- BT was forced to rely on the hosting defence as, unlike the other defendants, it hosted usenet groups and had the ability to remove postings. However, BT did not have the requisite "actual knowledge" of the postings complained of, and thus the defence succeeded.

The judge confirmed that the Godfrey case was right to say that the section 1 of the Defamation Act 1996 defence would be removed if the ISP had notice of the complaint, but suggested that rather more detailed knowledge might be needed on the part of the ISP if it is to be deprived of the protection of the e-Commerce Regulations. It may be therefore that the latter do provide stronger protection for ISPs than section 1 of the Defamation Act 1996.

Further information can be found in the document "Defamation and The Internet" by Charles Russell LLP dated 29 September 2006 on their website at - <http://www.crlaw.co.uk/>.

In 2006, in what is believed to have been the first case of its kind, the High Court awarded £10,000 in damages and over £7,000 in costs against a college lecturer who had made libellous statements on an internet bulletin board about a member of the UK Independence Party. The case - **Keith-Smith v. Williams** - QUEEN'S BENCH DIVISION [2006] All ER (D) 297 (Mar) illustrates the continued significance of online defamation and libel in the education sector. Details of the news story can be found on the Guardian Unlimited website at - <http://www.guardian.co.uk/law/story/0,,1737445,00.html>.

## Defamation, Liability, and Online Discussion Groups

Issues in terms of liability for offending content may arise in relation to discussion groups which function as online tutorials, monitored by a member of the institution's teaching staff.

The level of control exercised over such groups is of relevance. Typically, access will be limited to a small number of participating students and the tutor, with all answers being read and commented upon by the tutor.

In such a situation it is highly likely that the institution would fall within the remit of "editor", or "publisher", and thus not be entitled to rely upon the section 1 defence referred to above. This raises obvious problems, remembering that where sufficient editorial control is present, the institution becomes strictly liable for the content of the newsgroup / bulletin board.

The closed nature of the tutorial group makes no difference, as 'publication' of a defamation requires merely disclosure of the defamatory statement to one person other than the subject. This may seem a harsh approach in relation to an academic institution (as opposed to, for instance, publication in a publicly available newspaper), but it would seem to be the correct interpretation of the law in this context. It should, however, be remembered that any defamatory remark posted to a closed tutorial group is more than likely to be 'off-topic', and it should be a fairly simple matter, for an institution, to ban such posting and to delete messages not relevant to the discussion as a matter of course.

The ease with which a student in a closed tutorial group can be identified (not to mention any internal disciplinary procedures and penalties) should act as a strong deterrent to the making of defamatory posts.

It then becomes a matter of taking all reasonable steps to ensure the security of the system in order to prevent anyone not properly authorised from posting to the group.

**Source:** Lawrence Graham LLP - SmartLaw - Issue 49 - March 2007 - <http://www.lawgram.com/>.

Where institutions provide unmonitored online forums it is essential that it is clear to all users that they are required to comply with the institution's terms of acceptable use in the same way as they are with any other use of the institution's computer facilities. Clarifying and highlighting these terms of acceptable use is an ongoing responsibility for FE and HE institutions.

### 3. Terrorism

Under section 3(1) of the Terrorism Act 2006 the police can require providers of electronic services (including universities and colleges) to remove terrorist statements or articles which are hosted by them on the internet. If they fail to remove them without reasonable excuse within two working days of being requested to do so by the police, the institution may be deemed to have endorsed the statements and senior officers may be liable for criminal prosecution. The defences which exist as a result of the Electronic Commerce (EC Directive) Regulations 2002 (outlined above) will usually be available to the providers of electronic services in these circumstances.

#### **4. Responsibility for Obscene Publications**

Generally where individual students or staff engage in 'illegal' activity by means of an institution's communications system it is unlikely that the institution would be held liable except where office holders had actual knowledge of the unlawful activity (or their suspicions should have been raised and they took no action to prevent it).

However unlike other obscene material, the mere possession of child pornography is an offence in UK law. If a student or staff member is using space on the institution's computers to store child pornography, then the institution which owns the servers that it is hosted on could possibly be criminally liable for possession of that material.

There is an 'awareness-related' defence to such liability in the Criminal Justice Act 1988 (Section 160). Provided that the person in possession – the institution, or more specifically those employees responsible for management of the computer systems had not seen the articles in question and did not know that they were there, or had no reason to believe that they were in possession of child pornography, no liability will arise. Situations where this defence would not be available would be rare: typically those individuals who are determined to access and collect child pornography are very adept at hiding their material in information systems, and it is unlikely in the general run of things that the institution would expect to find such information being stored on its systems. Of course, the availability of this defence carries an implied obligation that as soon as the institution is notified of the presence of child pornography, it is immediately reported to the appropriate authorities – the police and also the Internet Watch Foundation (<http://www.iwf.org.uk/>).

See further 'FE/HE Institutions and Liability for Third Party Provided Content' - Gavin Sutter - <http://www.jisclegal.ac.uk/publications/thirdpartycontent.htm> and the detailed treatment of the area of Cybercrime on the JISC Legal website at - <http://www.jisclegal.ac.uk/>.

#### **5. Secondary Copyright Infringement**

##### **Infringement**

There are two kinds of copyright infringement, namely primary and secondary infringement. Primary infringement is direct infringement - doing or authorising an act restricted to the owner of the copyright ("restricted act"). Secondary infringement is indirect - selling or dealing in unlicensed copies or otherwise facilitating a primary infringement. The big difference between the two is that a mental element, such as actual knowledge or reason to believe that copyright had been infringed in making the infringing copies, is required for liability for secondary infringement.

Source - Intellectual Property and Information Technology Update - <http://www.ipit-update.com/> .

Copyright infringement can be a problem for an institution where any infringing copy is copied to college computers, for example, video or mp3 sound files without authorisation. It may also happen that staff or students use college webspace for storing infringing copies, for example, by means of peer-to-peer (p2p) file sharing facilities without authorisation. Does this mean that the institution will incur liability in respect of this infringing material?

In these circumstances the ingredients of secondary copyright infringement, s.23 of the Copyright, Designs and Patents Act 1988 (CDPA) have to be considered.

Unless the institution has clearly authorised the copying, the FE or HE institution is unlikely to be considered to be holding the infringing copies in the course of a business as the CDPA requires. The existence of files with extensions such as mp3 on the institution's servers should not necessarily be grounds for inferring knowledge of the infringement as a number of services allow users to download music tracks quite legally. A court is unlikely to expect a college or university to inspect every file on its servers and then to check whether it was legitimately downloaded.

In **Columbia Picture Industries -v- Robinson** ([1987] ChD 38), it was held that a general knowledge that some copies may be infringing did not constitute sufficient knowledge for secondary copyright infringement. (This case was decided under the equivalent provision in the previous Copyright Act of 1956.)

### **In Summary**

An institution is under a duty to take action once it has actual knowledge of infringing material on its computers or servers (such as by a notice sent on behalf of the copyright owner) or, through some other means, ought to have been alert to the likelihood of an infringement.

Further detailed treatment of the risks of secondary copyright infringement can be found in the paper "Legal Risks and Liabilities for IT Services in FE and HE" by Christine Cooper on the JISC Legal website at - <http://www.jisclegal.ac.uk/publications/legalRisks.htm>.

### **Removing Material from Publication - Free Speech**

Universities and colleges in England, Wales and Northern Ireland have a statutory duty to protect free speech by their members under section 43 of the Education (No.2) Act 1986 (similar provisions also apply to universities and colleges in Scotland). However where information published by a university or college, or one of its members, breaks the criminal or civil law (these are generally also breaches of the JANET Acceptable Use Policy) this duty may be overridden and the publication may be altered or removed.

## **6. Should an Institution Moderate Content?**

Those institutions that host content are often in a difficult position regarding how active they should be in taking responsibility for such content, and what legal liability they will incur by allowing staff and students to upload content for publication.

There is a very fine path for FE or HE institutions to tread between the requirement to take reasonable care in relation to publication and actually monitoring their users and their servers which would mean that they may face liability as a publisher.

The Electronic Commerce (EC Directive) Regulations 2002 do not address the imposition of a general obligation on service providers to monitor the information that they transmit or store, or to actively seek facts or circumstances indicating illegal activity. No such obligations exist in UK law, and their introduction would be incompatible with the requirements of the e-Commerce Directive.

However, this does not affect the imposition of monitoring obligations in specific cases (e.g. in compliance with a warrant issued under Section 5(1)(a) of the Regulation of the Investigatory Powers Act 2000 to secure the interception of a communication in the course of its transmission by means of a telecommunication system). Existing statutory obligations continue to apply equally online as well as offline.

Further detailed information on The Electronic Commerce (EC Directive) Regulations 2002 is available on the Department for Business, Enterprise and Regulatory Reform website at – <http://www.berr.gov.uk/>.

## 7. Conclusion

- Although it is usually the offenders, as individuals, who would face criminal prosecution or a civil action, an institution could suffer reputational damage if it is not seen to be acting responsibly.
- For institutions, as dispersed organisations, and, in an environment where electronic content can change every second, exercising control over the activities of staff and students in terms of what is published by them is likely to prove difficult.
- At its simplest, the more control the institution exercises over those who publish and upload information onto websites and online interactive forums, the more likely the institution will be held liable for any injury which those individuals cause.
- It is clear that receipt by an intermediary such as an FE or HE institution of notice of a defamation complaint is likely to remove key protections which UK law currently provides.
- An institution is under an obligation to ensure that users are not making illegal use of their internet and email access. This is best achieved with strict adherence to the JANET Acceptable Use Policy – <http://www.janet.ac.uk/services/publications/policy-documents.html>. Your institution must, for example, have in place policies to govern what topics and materials staff and students accessing the internet may use in blogs. Although a policy alone is unlikely to prevent misuse it does raise the issue to a formal level and enables an institution to take action against offenders as a disciplinary or employment matter.
- With the provision of message board facilities and the like it is likely that monitoring of each and every message is not required, but that any complaint about content must be responded to swiftly and the queried material removed. An institution should have a system in place to fast-track the removal of obscene, illegal, infringing or defamatory content from your computer networks once notified.
- This does raise concerns in respect of freedom of speech. Who is to decide what is, and what is not, offensive and/or untrue? How this squares with section 43 of the [1986 c. 61.] Education (No.2) Act 1986 (freedom of speech in universities and colleges) is, however, outside the scope of this paper.

## 8. Sources

Sources used in the compilation of this information include:

- FE/HE Institutions and Liability for Third Party Provided Content - Gavin Sutter - <http://www.jisclegal.ac.uk/publications/thirdpartycontent.htm>
- Legal Risks and Liabilities for IT Services in FE and HE - Christine Cooper - <http://www.jisclegal.ac.uk/publications/legalRisks.htm>
- Internet Watch Foundation (IWF) – <http://www.iwf.org.uk/>
- Internet Services Providers' Association, UK - <http://www.ispa.org.uk>
- Legal Aspects of Online Learning Environments - Gavin Sutter - [http://www.jisclegal.ac.uk/events/OLE\\_06/Programme.htm](http://www.jisclegal.ac.uk/events/OLE_06/Programme.htm)
- JANET - The UK's education and research network - <http://www.ja.net/index.html>
- Email - The Legal Issues - <http://www.weblaw.co.uk/art080998.php>
- Nick Armstrong - Society for Computers and Law Journal, September 2006
- Charles Russell - Defamation and The Internet - 29 September 2006 - <http://www.cr-law.co.uk/>
- Harassment / discrimination Managing the risks - Pinsent Masons - <http://www.out-law.com/page-450>
- Libel on the Internet?- Lawdit Solicitors - <http://www.lawdit.co.uk/>
- "A User's Guide to Copyright" Flint Tottel Publishing Sixth Edition 2006
- "ISP liability for defamation?" James Evans - Periodical Publishers Association - <http://www.ppa.co.uk/>
- Morgan Cole - HE and FE newsletter spring 2007 - <http://www.morgan-cole.com/businessareas/education/publications.html>
- Staff Misuse of the Internet - Times Online - <http://business.timesonline.co.uk/tol/business/law/article1155911.ece>
- Lawrence Graham LLP - SmartLaw - Issue 49 - March 2007 - <http://www.lawgram.com/>
- ISP liability for defamation? - Periodical Publishers Association - 06 Jun 2006 - <http://www.ppa.co.uk/>
- Intellectual Property and Information Technology Update - <http://www.ipit-update.com/>.
- Web content: The regulatory regime - Wragge & Co LLP - [http://www.wragge.com/legaladvice/commerce/default\\_11050.html](http://www.wragge.com/legaladvice/commerce/default_11050.html)
- The UK the Department for Business, Enterprise and Regulatory Reform website at – <http://www.berr.gov.uk/>.

JISC Legal - 23 November 2007

John X Kelly

© JISC Legal - [www.jisclegal.ac.uk](http://www.jisclegal.ac.uk)