Legal Risks and Liabilities for IT Services in Higher and Further Education

Universities and colleges might incur legal liabilities through the provision and operation of their IT facilities and may be interested in some practical guidance. Whilst not exhaustive, this paper attempts to bring together potential risks associated with the laws of contract and torts, employment law, privacy and data protection legislation and the newly emerging realm of Internet Law and Regulation. Liabilities arising from disability legislation and health and safety issues have not been considered.

1 Responsibilities to Students

1.1 The Nature of the Legal Relationship

It is now generally accepted that a contractual relationship exists between a university and its students and that statements in the prospectus and other publicity information may constitute terms of that contract. Information given to students about IT facilities must be accurate as the provision of a particular facility could persuade a student to choose a particular course. A claim for damages could result from the failure to provide that facility.

The legal relationship in a college of Further Education is less clear cut as students may have applied directly, through a third party (for example, a university franchise) or they may be under 18. This raises issues about who the contracting parties are. Even so, the Contracts (Rights of Third Parties) Act might still enable a student to enforce contractual terms directly.

Notices and Disclaimers in Prospectuses

Many prospectuses contain statements reserving the right to change the courses delivered, including the content of the course and the method of delivery. Whilst this may appear to protect the institution, it might fall foul of consumer protection legislation. A contract term is void (and so unenforceable) if, contrary to the requirements of good faith, it causes a significant imbalance to the parties' rights and obligations under the contract, to the detriment of the consumer[1]. The test of good faith might be quite difficult to satisfy if there were a substantial change in the nature and quality of the IT facilities actually provided from those described in the prospectus.

1.2 Breach of contract

If an institution fails to deliver the education promised or provides it in an inadequate way, then the student may be able to bring an action for breach of contract. The prolonged failure of some specific IT system that was essential to the delivery of a course could give rise to a claim. Failure of the systems supporting the Virtual Learning Environment, such as WebCT or Blackboard, would seem likely to fall into this category.

[1] The Office of Fair Trading is responsible for enforcing the regulations and has been willing to accept that students are consumers of educational services. The OFT Bulletins have reported a number of undertakings given by universities to change unfair terms in their regulations.

Liability might also arise where access to IT facilities is withdrawn from a student resulting in that student being unable to continue their studies. The student might have a strong claim for breach of contract if it is found that the regulation under which access was removed was unfair.

1.3 Actions in Negligence

To establish a claim in negligence, a student would have to show that a duty of care was owed to them by the institution, that the standard of care provided fell short of what was required and that some damage was suffered as a result. In most cases, the damage must be physical, although a purely financial loss can be claimed when there has been a negligent misstatement. Liability for a negligent misstatement could arise as a result of "expert" advice given on IT matters. A potential risk is advice given to students using their own equipment as inappropriate advice might render their equipment unusable and require a costly visit from an engineer. Staff must understand this risk even where they are students employed on a part-time basis.

Protection from Inappropriate Content/Harassment

Institutions have a duty to ensure the safety of their students and to protect them from any reasonably foreseeable harm. Liability could potentially arise for psychiatric conditions caused by repeated exposure to obscene or offensive material when using the institution's IT facilities.

Judging what is necessary to meet the required standard of care in this area is quite difficult. The National Grid for Learning advises schools that[2] "All schools have a responsibility to filter both access at school and any access pupils are given as part of home-school links." However, it also recognizes that "very restrictive filtering might be fine for use by primary children, but is likely to be inappropriate for out-of-hours use of computing facilities by older children or adults." Colleges of Further Education can have students as young as fourteen and a higher standard of care will be required to ensure their welfare.

Although there have been no reported negligence cases involving exposure to Internet content, the approach taken by the courts in negligence cases, generally, is to question the foreseeability of the harm occurring and the cost and/or effort involved in preventing it. The level of skill and specialist knowledge available within the institution will also be a relevant factor. Consequently, the standard of care expected in a university with highly skilled IT staff would be higher than in a small institution with a lower level of expertise to call upon. Also an institution that claimed to protect its users from inappropriate content may be held liable in situations where an institution that took fewer precautions would not.

Institutions should consider undertaking a risk assessment and feasibility study in this area. It may well be that the costs and difficulties involved in implementing an effective filtering system are prohibitive but this will not afford a defence if the assessment has not been carried out. Any general advice considered to be best practice in the sector should also be followed as this will help to establish that the amount of care taken was reasonable.

[2] "Internet filtering systems and filtering pupils' access on the Internet" available from http://safety.ngfl.gov.uk/schools/

It is also very important that there are accessible systems for students to report incidents and that effective means of preventing further occurrences are considered, such as changing their email address or giving advice on search techniques. After all, the case that is most likely to come to court is where a vulnerable individual has been repeatedly subjected to unpleasant experiences and numerous cries for help have been ignored.

2 Responsibilities to Staff

2.1 Fair Treatment

All employers must treat their staff fairly. If an employer fails to provide adequate IT equipment to enable a member of staff to carry out their duties properly, it could potentially support a claim of constructive dismissal.

If an institution is to discipline a member of staff for misuse of the IT systems, it is essential that there is an established policy communicated to all staff. Any action against an employee where there is no written policy clearly stating that a failure to comply will result in disciplinary action, up to and including dismissal, is liable to be held to be unfair by an Employment Tribunal.

2.2 Actions of Other Members of Staff or Students

Where a member of staff is accessing or downloading offensive images in a shared office, they may create an environment where colleagues feel harassed. The institution will be held responsible for this harassment if it does not take effective action when a complaint is received.

Staff working in open access computer areas might also be exposed to sexually explicit images being viewed or downloaded. In the US, a group of Librarians brought an action against Minneapolis Public Library after they were repeatedly exposed to pornography being viewed by library users. Failure to enforce acceptable use rules might result in a similar case in the UK.

Difficulties can arise when dealing with complaints in this area as there is no standard definition of what is offensive. Staff and students often like to use a favourite photo for their computer desktop which may upset those around them if, for example, it depicts a scantily clad model or an obviously homosexual couple. In such cases it is important to have a clear procedure for reaching a decision on whether an image is acceptable.

Protection from Inappropriate Content

Staff are subject to the same risks as students from inappropriate content and employers have a duty to protect them from foreseeable harm. Institutions should balance the cost and difficulty of implementing a filtering system with the likelihood of harm in the same way as for students.

3 Responsibilities to Third Parties

3.1 Actions of Staff

An employer is responsible for the actions of employees acting in the course of their employment. Universities and colleges are likely to be held responsible for emails and

other electronic communications sent by their employees in the course of their work and possibly also for other messages sent using the institution's systems.

It is important that staff understand that email carries the same legal weight as a letter on headed notepaper and that their emails may be used in legal proceedings. This can create liability for the institution if, for example, an email contains derogatory comments about a student or another member of staff. Where a defamatory statement could harm the business or reputation of a large corporation, damages could be substantial[3].

3.2 Actions of Students

A university or college will not generally be held liable for the actions of their students unless the institution had some degree of control over the behaviour complained of, or if the harm occurred as a result of the institution's negligence.

Liability for Students Downloading and Sharing Copyright Material

The development, over recent years, of systems which allow users to share files across the internet has lead to an epidemic of copyright infringements amongst young people sharing music and videos. A number of groups representing the interests of copyright owners have sought to take action first, against the developers of the file sharing software and, more recently, against individuals who are providing material for others to download.

Where the copying of the music or video is initiated by the student, the institution will not be liable for any primary copyright infringements. Simply providing the computers and networks that are being used to infringe copyright is also unlikely to raise liability. However, 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.

The existence of files with extensions such as mp3 on the institution's servers should not 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 university or college to inspect every file on its servers and then to check whether it was legitimately downloaded.

Any active participation in the breach of copyright will render the institution liable. Easy Internet Café was held liable where they operated a service to produce a CD of downloaded files. Institutions who provide a similar service for students, whether or not a fee is charged, should consider taking steps to ensure that material being copied is not subject to copyright. Where students have access to CD writers these should have copyright notices beside them similar to those beside photocopiers in libraries.

3.3 Liability for Content

Institutional Websites and Virtual Learning Environments

An institution will be liable under the Copyright, Designs and Patents Act 1988 for any copyright material appearing on the institutional website or in the Virtual Learning

[3] Norwich Union paid £450,000 to Western Provident Association to settle a case after a rumour had circulated on its internal email system about financial difficulties at Western Provident.

Environment (VLE). The act of placing it on the server will create a copy of the material for which the institution is liable, regardless of whether the existence of the copyright was known or not. This will be the case even where the new copy was transient or existed in memory only.

It is not always easy to determine whether material is subject to copyright. It is therefore important to limit the number of people permitted to publish material on the institutional website or VLE and to ensure that adequate training in copyright issues has been provided.

Links on university and college websites are also a potential source of liability. A link to a commercial site may need to be to the home page, rather than directly to the item of interest, if the site owner's revenue is dependent on the number of hits on the home page. A webpage containing a large number of links to pages within a particular site could be held to infringe the site owner's database rights under the Copyright and Rights in Databases Regulations.

Staff and Student Personal Webpages

Often facilities are provided for staff and/or students to create their own personal webpages that allow them to publish information about themselves and their interests. For staff, the extent to which the institution will be held liable for the content of these pages will depend on how closely the subject matter relates to their employment. It seems likely that the institution will be vicariously liable for almost anything that relates to academia or to their field of research.

Where the content relates to something not connected with their employment, such as a hobby, the institution is less likely to be held liable. However, once it has notice, it could still be held liable as a publisher of a defamatory statement or as a distributor of material that infringes copyright. In the Godfrey v Demon case, Demon was liable as the publisher of the defamatory material from the date they were informed that it was on their server.

Similarly, for students' personal webpages, it seems highly unlikely that the institution would be held liable except where it had actual knowledge of unlawful material (or its suspicions should have been raised) and it took no action to remove it.

Contents of Email

Emails might contain inappropriate material, personal data, defamatory remarks or viruses. Also they can easily be sent to the wrong address. Many organisations attach a disclaimer to email in an attempt to limit liability in some or all of these areas. Whilst it is not clear that liability can be excluded by unilateral notices, they can help to establish that an institution has taken reasonable steps to guard against some of these risks.

The harm caused by the dissemination of viruses by email might be considered foreseeable and, as damage to a hard disk is considered physical damage, it might found a claim in negligence. Having met the physical damage requirement, a claimant may also be able to recover consequential losses. Institutions should consider scanning outgoing email for viruses.

4 Information Security and Privacy

4.1 A Brief Overview of Data Protection

As this paper is concerned with legal risks and potential liabilities arising from the provision of IT services, it does not cover the requirements of the Data Protection Act comprehensively. Institutions should consult the JISC Data Protection Code of Practice[4] for general information.

Personal Data is any data that relates to a living individual who can be identified from that data. This includes information such as the record of logins on a computer as it can be matched to a real person. An IP address combined with a date and time might also be enough to identify an individual. The personal data collected in the course of normal operations by IT systems must not be used for other purposes without consent.

This personal data is considered to be sensitive (and so subject to more stringent requirements) if it relates to racial or ethnic origin, political opinion, sexual orientation or activity, trade union membership, health or criminal and alleged criminal acts. Email lists for certain groups, such as union members, implicitly contain sensitive data.

The Data Protection Act now also entitles a person to claim compensation if they have suffered damage or distress as a result of a failure to comply with the Act. This new liability is expected to bring an increase in the number of cases coming before the Data Protection Tribunal.

Respect for Privacy

Everyday system administration tasks will often bring IT staff into contact with personal information. It is rare for them to view the contents of private files or emails and most people understand the need for privacy in this situation. However, it may be less obvious that viewing the list of files in a directory or searching for entries in log-files also constitutes processing and requires the same respect for privacy. IT staff must be given appropriate training and guidance.

Collecting Personal Data

Where information is collected through a webpage it should state what the information is to be used for and should not ask for information that is not necessary. The use of cookies to collect information about users might be said to be unfair processing.

Personal data automatically collects in system log-files during the normal operation of IT systems. The length of time for which it is reasonable to hold this data will vary according to the type of data and the purpose for which it was collected. Institutions should have a documented Retention and Disposal Policy for data in log-files.

Publishing Personal Data

Liability may arise from publishing personal data. A directory of staff details may be published on the Internet without the need to get the consent of every member of staff. Staff and student email addresses and other contact details may also be published without the need for specific consent where access is restricted to members of the institution only. In all cases, people should be informed of what is being published and

[4] Available from www.jisc.ac.uk/uploaded_documents/dp_code.pdf

procedures must be put in place to remove an entry if it can be shown that publication would cause significant damage or distress.

Other information about identifiable individuals, such as photographs, should only be published when all reasonable efforts have been used to get consent. Sensitive personal information should only be published where the individual has given their explicit consent.

4.2 Information Security

One of the principles of the Act is that personal data must be secure. This means that appropriate technical and organisational measures need to be taken against unauthorised or unlawful processing. The level of protection required is proportionate to the harm likely to be caused by the unlawful disclosure or accidental destruction of that data. Institutions should have an Information Security Policy and the agreed levels of security should be monitored and reviewed periodically. Institutional Disaster Recovery and Business Continuity Plans should also consider the recovery of personal data, including that stored on desktop computers.

IT equipment which has reached the end of its usable life is a potential source of liability as the hard disk may contain personal data which must be safely destroyed. The use of laptop computers and home computers also poses a particular threat to information security as these are not subject to the same degree of control as computers on campus. Laptops are frequently stolen and home computers may be used by other members of the family, so additional measures must be used to protect any personal data.

4.3 Subject Access Requests

A Subject Access Request may require the disclosure of information in log-files, in email messages, in users' file store on a server or on the hard disk of a PC. An additional complication for IT departments is that personal data which has been deleted from the running systems might still exist on backup tapes and these might also need to be searched. If this would place an unreasonable burden on an institution, the person making the request may be asked to narrow down the search criteria.

To avoid liability to any third party who may be identified as a result of the Subject Access Request, (in an email for example), their consent should be requested prior to disclosure. If it is not received, any references to that person should be removed or obscured.

5 Acceptable Use Regulations and Investigations

5.1 Regulations, Awareness and Enforcement

Every institution should have an Acceptable Use Policy (AUP). To be enforceable, the AUP must be properly incorporated into the student contract or into an employee's terms and conditions and, additionally, reasonable steps must be taken to communicate its contents and any sanctions that might be imposed. It is important that the AUP is enforceable otherwise the institution may be held to have treated a member of staff or a student unfairly when taking disciplinary action.

5.2 Monitoring and Interception

The Regulation of Investigatory Powers Act 2000 (RIPA) makes it unlawful for the operator of a private communications system to intercept communications, other than in certain defined circumstances[5]. These provisions concern data while it is in transit; once it has arrived at the destination mailbox or server, interception law no longer applies and the data will be subject to data protection legislation and to the right to an expectation of privacy. Failure to comply with RIPA could result in criminal charges or a civil claim for damages.

The use of automated systems to scan for viruses (provided that the message is otherwise unchanged) and to filter Internet content is allowed. It is also permitted to monitor employees' email and Internet use to ensure compliance with policies and procedures but, before undertaking any monitoring, all reasonable efforts should be made to inform all parties that it will take place; this includes those outside the institution who may be affected. An impact assessment should also be carried out to ensure that monitoring is a necessary and proportionate measure to achieve the desired objective. The Office of the Information Commissioner has produced a good practice guide on Monitoring at Work[6].

5.3 System Administration Procedures

Systems administrators are sometimes called upon to investigate and gather evidence when there is an allegation of improper conduct. This could potentially give rise to liability for breaches of the Data Protection Act, the Regulation of Investigatory Powers Act or the Human Rights Act. It is essential that they understand their responsibilities and the limits of their authority. Documented procedures, making clear what staff are authorised to do (and what they are not), must be provided.

There is a risk that evidence gathered by IT staff during an investigation will be held inadmissible if it were gathered in an unlawful way. Evidence could also be discredited by the opposing counsel if presented inappropriately. The authenticity of email messages and the validity of login records are particularly likely to be challenged. Often university and college IT departments are unaware of these issues. Whilst they may receive guidance from the Police investigating a serious crime this will not be so for minor offences or for civil actions. Consequently, there is a risk that what may seem a cast iron case will founder at court. Expert advice should be sought at an early stage when considering proceedings.

5.4 Disclosure to Third Parties

Disclosure of information to a third party raises another potential source of liability. If the information is disclosed unlawfully, for example to a Police Officer without obtaining the appropriate paperwork, the institution could be held liable. It is therefore important to ensure that only a small number of people are authorised to disclose information and that they are adequately trained in the proper procedures.

A third party seeking the identity of a particular login name or email address, who does not have a right of access under any of the statutory provisions, can apply for a court

[5] These circumstances are defined in The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 available from www.hmso.gov.uk/si/si2000/20002699.htm

[6] "Employment: Part 3 – Monitoring at Work" available from www.dataprotection.gov.uk/dpr/dpdoc.nsf

order to get the information. As they will have to pay the legal costs, it is probably best, in most circumstances, not to disclose someone's identity without such an order.

6 Halls of Residence

6.1 Contractual Issues

Increasingly, network connections are provided to students living in Halls of Residence. Institutions charging a separate fee for this service have a contractual agreement with the student to provide the service, as advertised, even if there is no specific contract document. Ideally, there should be a formal agreement which covers what level of service is to be provided, what restrictions there may be and under what circumstances these restrictions may be imposed.

An institution does not have a right to access a student's own PC, even to scan for viruses or other vulnerabilities, without their consent. It may therefore be advisable to make that consent a condition of the connection agreement. It is important to ensure that the terms of the agreement are fair and reasonable as they will be subject to consumer protection regulations. For example, a term which prevented the student from claiming a refund even if the service were never delivered would be deemed unfair.

Where the IT service is not provided under a separate agreement, there might still be contractual obligations if it has been represented as forming part of the accommodation package. If this is not intended then it must be made clear prior to the accommodation agreement being signed.

6.2 The Institution as a Service Provider

Institutions providing a service to students in their accommodation may have some protection from liability if the institution's role in the unlawful activity falls within the definition of an Information Society Service Provider (ISSP)[7]. The protection applies to specific activities, not to the organisation in general and so will also apply where the unlawful activity takes place in a student computer room on campus.

Indications from the Department of Trade and Industry (DTI) are that intermediary service providers shall not be liable for damages or any criminal sanction as a result of transmission where:

(a) the information is the subject of automatic, intermediate and temporary storage, where the storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request; and

(b) the service provider:

(i) does not modify the information;
(ii) complies with the conditions on access to the information;
(iii) complies with the rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

[7] See "A Guide for Business to the Electronic Commerce Regulations" available from www.dti.gov.uk/industry_files/pdf/businessguidance.pdf

(iv) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(v) acts expeditiously to remove or to disable access to the information he/she has stored upon obtaining actual knowledge of the content being illegal.

There is no difference where students are using their own PC's plugged into the university's network, as it is the university's network that is transmitting the cached information.

Under the electronic commerce regulations, an ISSP has a defence against any civil or criminal action where they were a mere conduit through which a transmission took place; provided that they did not initiate the transmission, select the recipient or modify the information being transmitted. There is also a defence against actions arising from copying data into a cache provided that the copying is automatic, temporary and for the sole purpose of making future accesses more efficient. Again the information cached must not be modified.

The regulations provide the ISSP a further defence where a third party's unlawful material is unknowingly hosted on a server. An ISSP acting expeditiously to remove offending material, once it knows of its existence, is also protected.

Where an institution cannot use these defences, there is potential liability for copyright infringement when material is copied into a cache. This liability is strict so the institution is liable whether or not it had any knowledge of that material. There is also potential liability for distribution of copyright material or for publication of defamatory statements if these are made available by a student in a hall once the institution has actual knowledge or should have known.

7 Conclusion

Universities and colleges face liabilities in a number of areas as a result of providing IT services and some general strands have emerged. The need to deal with staff and students fairly is self evident and high standards of openness and transparency are clearly required.

The likelihood of damage or harm occurring is a central theme and this necessitates risk and impact assessments to determine what steps are best taken. The identification of best practice within the sector is also important here.

Actual knowledge is a key issue as it gives rise to liability under many heads. Although an institution needs to be alert, in most situations it will not be held liable for unlawful activities that it did not know about. The exception is the copying of material that is subject to copyrights.

The final theme is the need for documented policies and procedures covering the areas where liability might arise. Policies and procedures should be adequately communicated and need to be supported by appropriate training.

Summary of Recommendations

For ease of reference, the recommendations which appear throughout this paper have been loosely divided into four groups and ranked in (approximate) order of importance

within those groups. The section number(s) where they appear in the main text are also included.

Fair Treatment

- Have a written Acceptable Use Policy that is incorporated into staff and student contracts that clearly states what is and what is not acceptable. The AUP must also make clear what sanctions may be imposed if the policy is not adhered to. Remind all users regularly of the contents of the AUP and enforce it consistently. (2.1)
- Monitor communications only where an impact assessment has shown it to be proportionate and necessary. Take steps to inform all parties that the monitoring is happening. (5.2)
- Ensure that any personal information collected within IT systems is processed fairly. (4.1)
- Ensure that there is a specific agreement for the provision of IT facilities in Halls of Residence, even where no fee is paid. Ensure that the terms of the agreement are fair. (6.1)
- Ensure that the Prospectus and other pre-enrolment information contain accurate descriptions of the IT facilities and do not advertise services that are unlikely to remain available for the duration of the course. (1.1)
- All terms and conditions, including those in disclaimers and notices, must be expressed in plain English. If a term is detrimental to the student, it must be brought to their attention and the reasons should be explained. (1.1)

Risk and Impact

- Conduct a risk assessment and feasibility study to determine whether Internet content and emails should be filtered. (1.3 and 2.2)
- Identify any systems that are essential to the delivery of courses and make contingency plans for their failure. (1.2)
- Ensure that IT staff are cautious when advising students using their own equipment. (1.3)
- Consider using an email disclaimer and scanning out-going email messages for viruses. (3.3)

Awareness and Knowledge

- Avoid modifying data in transmission or when caching data whenever possible. (6.2)
- Train Systems Administrators in Data Protection issues. (4.1)
- Take extra care to determine whether material infringes copyrights when copying a student's files, especially if copying to CD for a student. (3.2)
- Limit the number of people who are able to publish material on the institutional web server or VLE. Provide training in copyright issues for this group. (3.3)
- Seek permission before linking to external sites from institutional web-pages. (3.3)
- Limit the number of people authorised to disclose personal information and train them in the proper procedures for lawful disclosure. (5.4)
- Consider how personal data stored on desktop computers might be recovered. (4.2)
- Take steps to ensure that people are aware of the legal standing of email messages. (3.1)
- Seek expert assessment of potential IT evidence to be used in any proceedings. (5.3)

Policies and Procedures

- Have efficient and effective procedures for removing unlawful material from systems when a notification of an infringement is received. (3.2)
- Ensure that there is an effective procedure for users to report incidents where they have found some content offensive. Consider measures to prevent further distress. (1.3)
- Have a procedure for determining whether an image, or other material, is offensive. (2.2)
- Have a written policy on what investigations system administrators may carry out themselves and when authority must be sought. (4.1)
- Document a Retention Policy for data in log-files. (4.1)
- Ensure that email stores and backup media are considered when responding to Subject Access Requests. (4.3)
- Develop and communicate a procedure for staff and students to opt-out of standard published directories. (4.1)
- Ensure that personal data is erased before disposing of redundant IT equipment. (4.2)
- Consider additional security measures for laptop computers and for users who work using their home computer. (4.2)
- Ensure that there is an adequate process for dealing with complaints that the IT equipment provided is inadequate or not functioning. (2.1)

Christine Cooper is Technical Infrastructure Manager at the London School of Economics & Political Science

September 2003

© JISC Legal Information Service 2003