

# Web 2.0 and the Law for IT Support Staff

18 September 2008

**Please note:** this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice.

## Table of Contents

1. Introduction .....	1
2. What is Going on? .....	1
3. The Risks .....	3
4. Boundaries for Users – Acceptable Use.....	3
5. What Needs to be Done? .....	7
6. Conclusion .....	8

## 1. Introduction

Web 2.0 technologies and resources change the way users communicate and interact. IT Support Staff are playing a central role in rolling out and supporting the next generation of technologies and practices. They are in the front line of policing and regulating usage, making on the spot decisions about security threats and attacks.

The new generation of students have different expectations and experiences which require new approaches and infrastructures to support their learning.

Institutions want to know how to take full advantage of Web 2.0 while ensuring that the legal risks are mitigated. This paper explores the particular legal difficulties which arise for those supporting the deployment and management of technologies and resources facilitating Web 2.0.

## 2. What is Going on?

One way to approach Web 2.0 is to look at the software commonly thought of as Web 2.0 software. Individual systems are hosted on servers and accessed across the web via a browser; they may be called Web 2.0 systems, Web 2.0 services or Web 2.0 applications. It is generally accepted that the innovation is changing the way people interact. Collaboration, contribution and community are the order of the day. Service provision can now take place anywhere, anytime with widespread use of mobile devices. International transfers and cross boundary access to information is the norm.

Traditional online environments limited users to viewing only, with publishers controlling content modifications. Web 2.0 applications allow the user to contribute content, including so called 'next generation technologies' such as blogs, social bookmarking services, wikis, podcasts, RSS feeds and social software which all provide enhancements over read-only

websites. This leads to a question of who owns the content?

Web 2.0 technologies will be used throughout the institution as part of the teaching and learning technologies deployed by teaching staff, or by individual users who sign up for online services which enable them to interact and share information with other users anywhere. In some institutions, blogs and wikis are promoted to staff as flexible tools for openness, creativity and community, to be used beyond application in learning and teaching.

Some of the Web 2.0 technologies used within FE and HE institutions include:

- **Wikis** - a wiki is a collection of web pages designed to enable anyone to contribute or modify content. Wikipedia is a good example of an existing resource created collaboratively. There are also blank wikis for collaborative work, such as those used for writing papers and research, communicating with students, post or pre conference collation of material and ideas. Wikis can be used to facilitate meetings – to prepare the agenda and deliver the minutes.
- **Blogs** - a weblog (blog) is an online journal which can be used to share, ideas, views, project status, or anything else you want. It allows a single author (or sometimes, but less often, a group of authors) to write and publicly display time-ordered articles (called posts). Readers can add comment to posts.
- **Free internet telephony** e.g. Skype, which facilitates voice, video and chat conversations online.
- **Instant messaging** accessed by web-based services such as Meebo and Trillian
- **Social personal web sites** (e.g. Myspace, YouTube, Gather and Bebo)
- **Collaborative working tools** for shared text production e.g. Google Docs and ThinkFree.
- **Social bookmarking** technologies such as del.icio.us (<http://del.icio.us/>) can be used to manage course reading lists in a collaborative way so that students can benefit from others' discoveries of relevant material. They can support development projects and research projects, allowing an information resource base to be constructed collaboratively.
- **Sites facilitating text and image sharing** such as Flickr<sup>21</sup>, Tabblo<sup>22</sup>, Our Story<sup>23</sup> & SlideShare<sup>24</sup>.
- **RSS feeds** for directing / receiving focused information
- **Mash-ups** - website or web application using content from more than one source to create a completely new or an improved service, such as RSS feeds for supplying content).

This list is not exhaustive because the technologies continue to proliferate.

### 3. The Risks

Scare stories in the media such as teachers and lecturers activities being published on YouTube, can create an air of concern about Web 2.0 – public scrutiny of personal activities has become a reality for many engaged in teaching and learning.

On the other hand many institutions have found that where there was some inappropriate use of blogs, for example, such postings usually disappear within minutes due to peer pressure.

### 4. Boundaries for Users – Acceptable Use

The first thing to remember is that users are already required to use any new technology appropriately. They must comply with the JANET Acceptable Use Policy which FE/HE will be familiar with. (<http://www.ja.net/>) New uses of the technology are covered in that unacceptable use is irrespective of the environment or the software used to carry it out.

Where students and staff engage in non curricular online activities using institutional computers it is essential that such activities are compliant with the terms of the policy. Any breaches should be responded to in line with the procedures outlined in the 'Acceptable Use Policy' of the institution. This should be technology neutral and apply equally to the Web 2.0 environment.

All FE and HE institutions have acceptable usage policies (it is a requirement for connection to JANET), but many go further and block a wide variety of ports and tools. In some

cases this is because of concerns over bandwidth usage (e.g. blocking Skype for fear of becoming a super-node and having undue network traffic). Some sites may be blocked because of concerns over "Malware" (viruses, trojans). Others have blocked services such as FaceBook and MySpace over concerns about legal responsibility for postings involving cyber bullying or defamation.

Getting the right balance between openness and safety, user needs and network security is important if Web 2.0 technologies are to become part of the learning tools of the institution. IT Support staff play an important role in fostering the culture which is necessary to facilitate innovation such as use of Web 2.0 technologies.

Legal areas which IT Support Staff should become acquainted with as they support Web 2.0 include:

#### Data Protection and Privacy – What the Law Says

The nature of Web 2.0 technologies places increased responsibility on institutions to safeguard the personal data which users entrust to them. The Data Protection Act 1998 (DPA 1998) applies to any personal data relating to any identifiable living individual. It includes data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions.

Staff and students can use blogs, wikis, online journals and diaries to share personal information. If this is hosted by the institution then the data protection legislation comes into play. Even just identifying people online can breach data protection legislation and

if the information disclosed is sensitive personal data then the breach is likely to be considered especially serious.

IT Support Staff are central to implementing and maintaining a culture of compliance with regard to data protection and the privacy of individuals. Security is a core responsibility. It is when exercising this responsibility that possible breaches of data protection and privacy may be disclosed.

IT Support Staff should acquaint themselves with the principles of fair and lawful processing of personal data and be alert to the risks for users when sharing personal data. For example, IT Support Staff should ensure users are made aware of the risks in disclosing so much information that they can be identified even if they do not use their name.

In addition staff should ensure users are aware that technology is not always secure and corruption and interception (intentional and unintentional) of data does occur.

The DPA 1998 requires that personal data should not be kept longer than necessary. Where external Web 2.0 services are used it should be ensured that adequate data privacy safeguards are in place which guarantee the removal and disposal of users' personal data after the purpose for which it was collected and processed has ended.

Institutions should be careful about compelling users to sign up for Web 2.0 services which require them to consent to Terms and Conditions. Institutions should, when inviting users to register for a Web 2.0 service, provide clear guidance about the data protection implications of that

registration; provide advice on the effective use of privacy enhancing elements of the service; and guidance on how to unsubscribe and remove personal data from the service. IT Support Staff can play a key role in this awareness raising by assisting users to understand their processing choices in terms of what items are compulsory and what are voluntary when filling out online forms.

### **Copyright – Liability for Infringement – What the Law Says**

Web 2.0 applications allow users with little web skills to put their own, or third part content, online thus encouraging social networking and development. Content is portable and re-using and re-mixing easier. Even though it may not always be clear where ownership lies, the law of copyright will still apply to this content.

Copyright infringement can be a problem for an institution where any infringing material is copied to college computers without authorisation e.g. video or mp3 sound files. It may also happen that college web space is used for storing infringing copies, for example, by means of peer-to-peer (p2p) file sharing facilities. This does not necessarily mean that the institution will incur liability in respect of this infringing material.

Special difficulties may arise when infringing materials are incorporated into teaching materials. 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 legislation requires.

## **Discrimination against those with Disabilities – What the Law Says**

Under the terms of the Disability Discrimination Act 1995 (DDA) it is unlawful for any FE or HE institution to discriminate against a disabled student in relation to teaching, assessment and access to learning resources, course materials, websites, VLEs and computer facilities.

IT Support Staff play a significant role in preventing any substantial disadvantage arising for those individuals with disabilities. This includes access to and use of technologies which are compulsory for a course. JISC TechDis are able to help institutions ensure that their obligations in this area are fulfilled - <http://www.techdis.ac.uk/>.

## **Liability for Content – Defamation – What the Law Says**

IT Support Staff may come upon computer content which is offensive towards particular individuals.

Defamation is 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. This applies to FE and HE institutions as publishers in the same way as to any other publisher. 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.

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 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.

Once notice of a defamation complaint is received the institution should investigate immediately and remove the offending material as that notification generally removes key protections which UK law currently provides.

The defence of 'innocent dissemination' of a defamation is available to staff 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

## **Where Users Upload Copyright-infringing or Defamatory Content – What the Law Says**

If the institution did not know about it and acts to take it down as soon as it is made aware of it, the institution will not be held responsible. However where the institution moderates content and misses defamatory content, the institution could be taken as the publisher and be held responsible. Procedures should be in place to take down offending material once notice has been received of infringing content.

## **Publications of Obscene and Illegal Materials – What the Law Says**

Institutions will not be held responsible if they did not know about the material and act to take it down as soon as made aware of it. Where institutions moderate content and fail to prevent the content being published they could be taken as the publisher and be held responsible. Likewise in these circumstances procedures should be in place to take down offending material once notice has been received of infringing content.

## **Bullying, Harassment, Stalking – What the Law Says**

IT Support Staff have an important role to play in fulfilling the institution's obligation to provide a safe environment for their users in the context of Web 2.0. Such incidents may come to light as a result of routine monitoring and maintenance by IT Staff or as a result of a complaint. Clear incident handling procedures must be in place to ensure incidents are investigated appropriately, and evidence gathered and presented which can help establish the innocence or guilt of those involved.

Harassment by email or online is a serious concern. The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which that person knows, or ought to know, amounts to harassment of another. This includes by email or by other computer related means such as discussion forums, or social networking.

In England and Wales under s.1 of the Malicious Communications Act 1988 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person. Under s.43 Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent offensive or threatening. Both offences are punishable by imprisonment and/or a fine.

In Scotland cases of online intimidation and harassment offences are likely to be dealt with as breaches of the peace.

Legally, as employers, FE and HE institutions have a common law duty of care, as well as responsibilities under health and safety and discrimination legislation and need to take action to prevent harassment. This involves encouraging incidents to be reported, responding promptly and ensuring policies are followed correctly. IT Support Staff have a key role to play in ensuring that information technology facilities, including Web 2.0, are not used for bullying, harassment or stalking.

## Summary

- It is important for IT Support staff to ensure that any potentially legal problems with Web 2.0 technologies are dealt with swiftly
- Contingency plans should be in place to ensure that illegal content on institution computers is removed as soon as possible including anonymous comments.
- Institutions are required to keep enough information in order to be able to trace any use of the JANET (<http://www.ja.net/>) network to specific computers or individuals. JANET and law enforcement agencies may request to see these logs. JANET does not expect institutions to retain logs for more than three months
- Before signing up to a Web 2.0 service provider which involves the processing of user personal data, IT Support Staff should consider whether the terms of use and facilities of the external service will enable them to do take down and delete offending material quickly

## Example

Your institution receives notification that material on an external social networking site contains racist remarks. The comments involve stirring up hatred against persons on racial or religious grounds and are identified as originating from your institutions network.

IT Support Staff need to be able to trace the activity to specific computers and identify individuals. The notification should trigger an incident response procedure which comes into effect and which removes the offending material.

## 5. What Needs to be Done?

IT Support staff must judge and monitor the legal risks for the individual and the institution as Web 2.0 technologies become more central to activities.

### Example

The institution receives notification that material on a blog hosted by a department is offensive and insulting to a particular user. IT Support Staff need to be able to respond by isolating the material and removing it once this is sanctioned by the institution's authorised person.

### Authorised Person

Your institution ought to appoint a person or persons who will be authorised to decide when content is inappropriate. They act on behalf of the institution and may be members of the institution's management team. They should be appointed in accordance with the appropriate management procedures within your institution which may, for example, take the form of a Scheme of Delegation.

### Staff Training

Like any group of individuals IT Support staff will be made up of those who are early adoptors and technology enthusiasts as well as those who are more reluctant and dubious about new ways of working.

Keeping up to date with how users are using the technology is an ongoing process and is a necessary part of the skills required by IT Support staff.

## 6. Conclusion

Whether we like it or not Web 2.0 is changing the way information technology is used. It brings greater user control and ease of use.

The potential of Web 2.0 for FE and HE is just starting to be explored - the possibilities of using these technologies to deliver teaching materials and enhance interaction between teachers, administrators and the students are numerous.

The virtual environment can be a more permissive one, with open communities engaged in learning activities co-existing with business models. However, as in the real world, the legal issues need to be identified and managed.

Web 2.0 systems are increasingly being used on an individual course module level, and at an institutional level. The introduction of Web 2.0 systems is not unproblematic, as there are ramifications in the areas of type of system for institutional use; external or institutional hosting; integration with institutional systems; accessibility; visibility and privacy; data ownership, IPR and copyright for material created and modified by college members and external contributors; control over content; longevity of data; preservation; information literacy; staff and student training; and appropriate teaching and assessment methods.

Clearly it is necessary to balance the need for legal compliance with a light-touch approach in the use of regulations that might constrain experimentation with the technologies and allied pedagogies.

## Acknowledgements - Sources

1. Web 2.0 and IPR - A short scoping study for the Users and Innovation Programme, JISC - Naomi Korn and Charles Oppenheim - April 2007 - <http://www.jisc.ac.uk/media/documents/projects/scopingpaperweb2oandipr2nddraft.pdf>
2. Web 2.0 for Content for Learning and Teaching in Higher Education - <http://franklin-consulting.co.uk/LinkedDocuments/Web2-Content-learning-and-teaching.doc> - 28 May 2007
3. Game-based Learning Briefing Paper - JISC - May 2007 - [http://www.jisc.ac.uk/publications/publications/pub\\_gamebasedlearningBP.aspx](http://www.jisc.ac.uk/publications/publications/pub_gamebasedlearningBP.aspx).

**18 September 2008**

**JISC Legal**