

Web 2.0 and the Law for Information Services



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. Outline of Risks and Liabilities	1
3. Risks and Liability Associated with Personal Data	1
4. Risk and Liability for Copyright Infringing Content.....	3
5. Risk and Liability for Inaccessible Content	4
6. Risk and Liability for Defamatory and Obscene Content	5
7. Steps Towards Risk Mitigation.....	6
8. Citations and Bibliography	7

1. Introduction

Institutions, including their information service departments, are fast moving to adopt Web 2.0 technologies as they recognise the potential value to their activities. The types of web 2.0 technologies popularly used by information service departments include blogs, wikis, social networking sites such as Facebook, online communities such as Second Life, podcasts, instant messaging and RSS. Apart from this, information services are also developing their own web 2.0 based applications to support learning, teaching and research. This for example, would include applications like Copac or Intute.

Information service managers deploying or managing technologies and resources that support Web 2.0 should therefore be clear on their responsibilities and duties towards staff, students and other users affected by it. This would require that they give due consideration to the array of risks associated with Web 2.0 technologies and work out risk mitigation and management techniques to minimise liability.

This overview paper points out some of these risks and liabilities. The paper also suggests some risk mitigation steps which institutions could consider in order to minimise liability and manage risks relating to Web 2.0.

2. Outline of Risks and Liabilities

The legal risks and liabilities associated with the use of Web 2.0 technologies by information service departments include:

- Risk and liability concerning personal data
- Risk and liability relating to copyright infringing content
- Risk and liability for content inaccessible to disabled people
- Risk and liability for defamatory and obscene content

3. Risks and Liability Associated with Personal Data

Many web 2.0 technologies place users at a point where submission of personal data is necessary to use the tool. This brings

with it risks concerning the privacy and personal data of individuals. Information services staff might use Web 2.0 technology through social networking websites. These websites support applications like Facebook or MySpace. Members of staff might create personal or official accounts through such applications. Professional accounts could include ones that are created by libraries. For example, a member of library staff might create an account to support networking with members in the same library or with those outside the institution. The profiles created in such accounts could contain both personal and official data. The personal data might comprise names, date of birth, photographs and other biographical details of its users. Apart from this, staff might also reveal other personal information such as details on their day-to-day life or relationships by means of posting messages.

In the case of official accounts, it could happen that a member of staff is involved in maintaining the account. When a new user makes friends with this member, his profile and personal information could become available to users who are friends of the member. Although altering the privacy settings in the application could preclude access to certain personal information, it might not be fool-proof to prohibit complete access to the personal data of a member.

In some cases, members of staff may also operate an official account through a single login. If the login and account details are exchanged to other members of staff it could provide easy access to the personal details of a member of staff.

Where Web 2.0 applications are developed or deployed by information services departments and where personal data relating to individuals is collected, institutions need to be aware of their duties and responsibilities and the rights of their data subjects (staff, students and other users of web 2.0 affected by it) under the Data Protection Act 1988 (DPA). Any obtaining, holding, using, processing and disclosing of the information relating

to individuals should be within the remit of the principles of the DPA. If not, there is a risk of being held liable for breach of the DPA.

Information service departments need to adhere to more stringent conditions when processing sensitive personal data. Section 2 of the DPA refers to sensitive personal data to mean 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. Therefore, where departments process the sensitive personal data, for example, collect information or details regarding a person's ethnic origin or religious beliefs, sex life etc in order for them to use a Web 2.0 tool, explicit consent from the users should be obtained prior to processing any sensitive personal data.

Processing of data for marketing and advertising purposes is one other risk which departments need to be aware of. Such a risk could arise in situations where the personal data collected for or during Web 2.0 use is used for purposes of advertising or marketing. It should be understood here that users have the right to object to this and therefore they should be given the option to opt out of being exposed to such marketing or advertising material.

Of note is also that one of the principles (fifth principle) of the DPA obligates the data controller to keep the data only for the time for which the information is necessary to perform the operation for which it was collected. Information service departments operating Web 2.0 applications or accounts where personal data is collected thus need to ensure that the data collected in such accounts is used only for the limited purposes of operating the library tool.

Risks associated with personal data include:

- Unintended release of personal data by the user
- Inadequate privacy settings on the system
- Potential breach by the institution of the DP rights of the data subject
- Not providing users the right to opt-out from advertising and marketing material

4. Risk and Liability for Copyright Infringing Content

Web 2.0 based Wikis are a useful resource for libraries and information services. They are developed through collaborative writing and with contributions from a number of people. It could comprise the academic members and students who use the wiki provided by information services department and the information services staff themselves, who both contribute to and maintain the tool. The wiki serves the role of an information resource and as a publishing platform. This could create risks concerning the legal validity of the information contained in them.

Information services departments operating wikis could act as both users and publishers of content. This could take the form of staff adding, removing or editing content which in some cases may be without the consent of a registered user. For example, researchers at institutions might want to add content or information or offer their notes for inclusion in the catalogue and other online resources.

Where a department lacks the resources to verify the accuracy or completeness of the information or to edit the content prior to uploading it into the wiki, there is a risk that the content submitted is inaccurate or misleading. Although this problem could be alleviated by means of peer review prior to submission, the potential legal risks arising in such situations would far outweigh these. Adaptation of content is one such legal risk. Adaptation of content

may be necessary for proper upkeep of the wiki. But it should be noted that the right to adaptation is one of the exclusive rights of the copyright owner and therefore any adaptation should be with the permission of the copyright owner. The other means to minimise liability against risks related to incorrect information would be to display disclaimers on the websites that host Web 2.0 technologies. The disclaimers could be used to limit the liability of the institution when users use the Web 2.0 technology and act based on the information provided in it.

With a number of contributors to the tool, the content in the wikis could involve a number of authors and as a result create single or multiple copyright owners. If each author were to claim copyright in their individual contribution, it could create disputes relating to copyright ownership. Collaborative creations in wikis can involve a multitude of combinations in terms of the creators involved. Staffs, students, members of staff from various institutions, visitors to the institution, employees from funding organisations and industrial sectors could all form a part of a collaborative research group. Here people might share resources ranging from equipment and facilities to intellectual and research capabilities. One of the most common IPR issues here is the individual right to authorship and copyright ownership in content contributed by one person as against the other. A student who contributes to a common data pool might also wish to claim ownership in the submitted content. It could however be the case that the submitted content incorporates material that is inseparable and is created by other members of the team or a faculty member. Considering such risks, it is imperative that the institution gives due consideration to the development of staff and student intellectual property rights policies and incorporate provisions on IPR ownership in staff contracts of employment prior to facilitating Web 2.0 technologies at institutions.

Content contributed by authors might also comprise third-party copyright material or even orphan works (works in which the rights holder cannot be traced or are unknown). Appropriate copyright clearance or permissions are necessary to post these materials in the wiki. Where such clearance or permission is lacking the institution could face the risk of being sued for hosting copyright infringing content. This could also indirectly affect the proper running of the wiki.

Issues similar to those encountered when facilitating wikis could arise with regard to Web 2.0 technologies offering 3D virtual environments. Second Life serves as a good example in this regard. Institutions or information service departments might buy islands in 3D worlds like Second Life. This could be for purposes of providing reference services, sharing information, running meetings, performing surveys, obtaining comments or even for hosting public discussions on specific topics. The library at University College Dublin (the first Irish library in Second Life) providing “reader survey, query box service, blogs, presentations and e-book” and Infolit iSchool are some examples. The virtual objects created by users in Second Life are copyright and users might copy another person’s content, build or design and then display it on other islands. This creates issues of copyright infringement at various fronts – copyright infringement by copying, communicating, adapting content and also where the copied content involves derogatory treatment of an ‘avatar’ or object issues pertaining to infringement of the moral right. And with the institution providing space or facilities for using second life, claims could also be raised against the institution for authorising infringement.

Risks associated with adding content include:

- Copying, adapting and communicating contents without permission
- Adding, removing or altering material without permission
- Inaccurate or misleading content
- Difficulties identifying an author for subsequent changed treatment of content
- Multiplicity of authors could lead to disputes over copyright ownership

5. Risk and Liability for Inaccessible Content

Information services offering learning resources or services for students should consider the effect the laws on accessibility have in relation to the provision of services. The primary legislation in relation to accessibility is the Disability Discrimination Act of 1995 (DDA). The scope of the DDA was extended to include education services by the Special Educational Needs and Disability Act 2001 (SENDA). Part III and Part IV of the DDA is applicable to education services. This would include the further education, higher education and specialist education sectors.

The DDA prohibits discrimination against disabled people in a range of circumstances and includes employment, education and the provision of goods, facilities and services. Only those people who are defined as ‘disabled’ in accordance with section 1 of the Act are entitled to the protection that the Act provides.

According to the Act a disabled person is a person who has an impairment that is either physical or mental, and the impairment has adverse effects that are substantial and long-term, thereby affecting his/her normal day-to-day activities. The breadth of the definition will cover a majority of disabled people who have barriers on accessing or using services offered by an institution.

Under section 28 of the DDA, the institution is under a duty to make

reasonable adjustments so that the disabled student is not at a 'substantial disadvantage' when compared to those who are not disabled. This duty would arise in relation to student services.

The term 'student services' refers to "any service that an education provider provides, or offers to provide, wholly or mainly for students." Some of the examples of student services include "learning equipment and materials such as laboratory equipment, computer facilities, class handouts, etc and libraries, learning centres and information centres and their resources." Therefore, information service departments should make sure that the services offered by them through web 2.0 technologies are also accessible to the disabled staff or students. For example, this could include situations where libraries services are imparted by means of podcast, e-portfolio systems for students operated by means of blogging software, or running of library courses via blogs. Here, a duty is imposed on the department or the host institution to make reasonable adjustments to these services so that disabled students are not placed at a substantial disadvantage. More information on the factors relating to 'reasonable adjustment' can be obtained from the Code of Practice (revised) for providers of post-16 education and related services (see the Commission for Equality and Human Rights website at: <http://www.equalityhumanrights.com/>).

Risks associated with inaccessible content:

- Potential breach of obligations under the DDA causing disadvantage to disabled students
- Failure to meet duty to make "reasonable adjustment" if use inaccessible Web 2.0 functions

6. Risk and Liability for Defamatory and Obscene Content

Being a medium for expression of thoughts, blogs constitute one of the classic Web 2.0 technologies that could

create liability for inaccurate, defamatory and obscene content.

Although the evidence of an information service or library blog being used as a medium for such actions is yet unavailable, the department or the institution could be held liable if staff post content that is defamatory or obscene on these blogs.

The relevant law on defamation in the UK that would apply to blogs is the Defamation Act 1996 (the Act). The Act applies to print media and to publication over the internet. Published content is defamatory and untrue if it "tends to lower a person in the estimation of right thinking members of society generally; or which tends to make them shun or avoid that person." Libel is a cause of action for defamation and refers to publication of defamatory content in permanent form and so would include online publication in blogs. The content could include postings made on a blog, or even comments passed by users of the blog on specific postings. Therefore, content managers (information service managers or staff managing the blog) could be liable for defamation if the content hosted in a blog is defamatory and if steps are not taken to remove the defamatory material being removed from the blog. Defamatory content on blogs could also pose legal issues for the institution in the sense of being held vicariously liable for actions of their employees. Circumstances such as these could arise where the institution had authorised the conduct of an employee at the institution. It would however exclude situations where the action of a member of staff was outside the activity authorised by the university. This for example can be a situation where a member of staff operates a personal blog from his home and posts defamatory comments on them.

With regard to obscene content posted on blogs, information services need to be aware of what actually constitutes 'obscene' content. The legal definition of 'obscene' is narrower than the dictionary meaning and is set out by the Obscene Publications Act 1959 and 1964 (OPA).

The Act makes it an offence (punishable with up to 3 years imprisonment or an unlimited fine or both) to publish an obscene article or to have an obscene article for publication for gain. Under section 1(1) of the OPA, a material is considered 'obscene' if it has the tendency to deprave or corrupt those likely to be exposed to it. This wide definition would include other material rather than just sexual depictions posted on blogs. Thus, an offence of obscene publication in relation to a blog could be committed simply by making obscene material available for electronic transfer or downloading by another party who is thus enabled to access and copy that material. Content managers will thus need to make certain that contents and comments posted on blogs are not obscene or that which will bring the institution into disrepute.

Of note with regard to publishing of obscene content is also the recent legislation, the Criminal Justice and Immigration Act 2008, which among other things has increased the sentence for publishing an obscene article. Under the Act, sentence for publishing of an obscene article has been increased from 3 to 5 years imprisonment.

It merits consideration to mention here that virtual worlds like Second Life could also serve as platforms where the institution or information service departments might face liability for content that is defamatory or obscene. This could arise in situations where users for example make comments that are defamatory or share clips, animations or other content that might be obscene.

Risks associated with defamatory or obscene content include:

- Blog contributors publishing defamatory materials could make institution liable by association
- Inadequate "notice and take down" procedures for offending material
- Potential breach of Obscene Publications legislation
- Potential damage to institutional reputation

7. Steps Towards Risk Mitigation

1. Information services operating and supporting Web 2.0 technology would need to support its use with a 'terms of use' or acceptable use policy (AUP) policy. Emphasis should be placed on the clarity of the policy - it should be clear to users what they can and cannot do when using web 2.0. This might for example, be in terms of imposing restrictions on their use.

2. If an institution has an existing policy, it should review the policy to check if it is fit for purpose and covers Web 2.0 use at the institution. Consultation should be arranged with departments using Web 2.0 applications on their current policy arrangement. The extent to which the goals of the policy are being met should be ascertained.

3. Staff and students should be made aware of their rights and responsibilities when starting to use a Web 2.0 technology.

4. Prior to deploying Web 2.0 technologies, appropriate confidentiality agreements should be entered into with third parties with regard to transfer of personal data over Web 2.0. The users of Web 2.0 should be given information on the parties to whom their data will be disclosed, and the policy should contain appropriate provisions for this.

5. Institutions must also include in their policy a clear procedure to be followed in cases of dispute relating to Web 2.0.

6. Most importantly it should be ensured that any policy or agreements are complied with and that any use is within the bounds of these.

7. Where an institution hosts Web 2.0 applications, content managers acting on behalf of their institution could be held liable for copyright infringing, defamatory or obscene content

published in them. Content managers should therefore scrutinise content to see if appropriate rights clearance has been obtained prior to uploading them on wikis or blogs. Necessary and relevant editorial control should also be exercised on Web 2.0 applications such as blogs to ensure that content posted is not defamatory or obscene.

8. It should be remembered that the legal duty of designing a Web 2.0 application to aid disabled people extends to services provided by and operated by educational institutions for their students. Therefore, institutions should be mindful of their duties under the DDA.

8. Citations and Bibliography

- Delasalle J. (2008), “*Web 2.0 – Help or Hype? – Social Softwares and their value to Libraries*”, Web 2.0 and the Library and Information Service, *ALISS Quarterly*, Vol. 3 (2), January 2008
- Lyn Parker, “*More Questions than Answers: The Reflections of Maggie Kohime, A Virtual Librarian in Second Life*”, Web 2.0 and the Library and Information Service, *ALISS Quarterly*, Vol. 3 (2), January 2008
- The Data Protection Act 1998 available at <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>
- Your Archives available at <http://yourarchives.nationalarchives.gov.uk>
- Copac available at <http://copac.ac.uk/>
- Intute available at <http://www.intute.ac.uk/>
- University College, Dublin Branch libraries available at http://www.ucd.ie/library/about/branch_libraries/index.html
- Infolit iSchool <http://cilass.group.shef.ac.uk/?p=229>
- Grannum, G., (2008), “*Your Archives*”, *ALISS Quarterly*, Vol. 3 (2), January 2008
- Report of the Information Services working Group on Collaborative Tools, (2006), “*Collaborative Software Tools and Web 2.0*”, University of Edinburgh, Edinburgh, available at <http://www.vp.is.ed.ac.uk/pub/jsp/polopoly.jsp?d=290&a=1167>
- Disability Discrimination Act Department of Work and Pensions, (2006), “*Consultation Document: Guidance on matters to be taken into account in determining question relating to the definition of disability*”, TSO, London, available at <http://www.dwp.gov.uk/consultations/2005/disability.asp>
- Disability Discrimination Act 1995 (DDA) available at - <http://www.opsi.gov.uk/acts/acts1995/1995050.htm>
- The Special Educational Needs and Disability Act 2001 (SENDA) - This legislation amended the DDA to include education services as Part IV of the DDA available at <http://www.opsi.gov.uk/acts/acts2001/20010010.htm>
- Disability Rights Commission, (2007), “*Code of Practice (revised) for providers of post-16 education and related services*”, TSO, London, available at http://83.137.212.42/sitearchive/drc/pdf/COP_Post16.pdf
- Defamation Act 1996 available at http://www.opsi.gov.uk/Acts/acts1996/ukpga_19960031_en_1
- *Sim v Stretch* (1936) 52 T.L.R 669
- The Obscene Publications Act 1959 (OPA 1959) available at <http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1128038>
- *R v Anderson & Others* (1971) 3 All ER 1152
- Criminal Justice and Immigration Act 2008
- http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1
- Sutter, G. (2003), “*FE/HE Institutions and Liability for Third Party Provided Content*”, JISC Legal, Glasgow, available at http://www.jisclegal.ac.uk/publications/third_partycontent.htm
- For recent UK case law relating to defamation and publication over the internet refer to - *Loutchansky v Times Newspapers Ltd & Others* [2002] 1 All ER 652

18 September 2008

JISC Legal