

# Web2Rights

## Other Legal Issues Factsheet

### **Defamatory, obscene and other unlawful content**

Of particular concern to the providers of next generation technologies may be the potential liability for hosting infringing material (for example if contributors post defamatory or obscene material or works which infringe copyright). The E-commerce Directive and Regulations provide for some immunity against liability for a service provider which hosts, caches or acts as a conduit for unlawful content so long as certain criteria are met. Broadly the service provider who hosts or caches unlawful information will not be liable for damages or for any other pecuniary remedy or for any criminal sanction so long as they do not have actual knowledge of the unlawful activity or information and is not aware of facts or circumstances from which it would have been apparent that the activity or information was unlawful. Neither should the service provider have had a hand in transmitting or in any way altering the information. Please note that the E-Commerce Directive and Regulations do not apply to ISP's located outside the European Union. So if the plan is to use an ISP located in the US, make sure that the service complies with the legislation of the country where the ISP is located.

Although the rules are somewhat complex (for instance they do not state what is meant by expeditiously, nor how actual knowledge is obtained by a service provider), in general service providers have sought to mitigate liability that might arise by putting into place a notice and take down procedure and by making the service subject to specific terms and conditions (which usually exclude liability of the service provider. Such terms and conditions can be found on the website of the service provider. Most notice and take down procedures provide that when a service provider receives notice that allegedly infringing material is on the site and/or on the equipment operated by the service provider, then the material is removed. While instituting such a procedure is good practice, there are factors that providers of Web 2.0 technologies within the academic sector might like to consider:

- The procedure for taking down allegedly infringing material. Will any investigation be made as to the identity and provenance of the complainer prior to removing the material?
- Put-back Procedure. Will the service provider consider instituting a 'put-back' procedure whereby the material is automatically re-instated should it be found to be non-infringing?

Courts in a number of jurisdictions are starting to require service providers to install filtering software (dealing notably with material that infringes copyright) in order to maintain immunity from suit. Whereas liability in these cases tends to arise where the provider of the next generation technology is profiting from a business model that infringes copyright belonging to third parties (such as a service that makes clips of videos available profiting from advertising revenue) some thought might be given to the possibility of building filtering tools in educational Web2.0 technologies.

### **Data Protection**

If you are developing a next generation technology and will be dealing with information about individuals then you will need to consider the Data Protection Act 1998. This Act applies to personal data about living, identifiable individuals. Thus if you collate information about users of the Web2.0 technologies (for instance students contributing to a collaborative learning environment) which might include name, address, age, student number (which can then be linked with the name of the student elsewhere) then the terms of the Data Protection Act will apply.

The Act imposes obligations on the data controller. A data controller is the organisation that makes the decisions as to how and why personal data is to be processed. Processing data includes

# Web2Rights

reading, using, amending, storing and deleting the data. Even where the information is passed to a third party to be processed, the data controller will remain liable for the obligations under the Data Protection Act where the controller is the entity that specifies what should be done with the data during processing. If you develop a Web2.0 technology and use store and/or delete information about the users then it is likely to fall under the definition of data controller.

## *Data Protection Principles*

The Act requires the data controller to act in accordance with eight principles

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## **Sensitive Personal Data**

Where personal data becomes 'sensitive' then the data controller has additional responsibilities. Data becomes sensitive if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life
- commission of offences or alleged offences

Where processing is of sensitive personal data then, in general, consent to processing must be explicit. When using web2technologies in the educational environment it may be that the contributors to the project and/or the users of the technology disclose sensitive personal data as part of the educational experience. If this is likely to be the case, then explicit consent of contributors should be obtained to processing of the data.

The same project plan developed for the purposes of defining the copyright strategy can be used to define a data protection strategy. For a most useful Data Protection Compliance Check List see [http://www.ico.gov.uk/upload/documents/pia\\_handbook\\_html/files/DP%20checklist%20final.doc](http://www.ico.gov.uk/upload/documents/pia_handbook_html/files/DP%20checklist%20final.doc)