



## **Legal and Regulatory Issues for Intranet Managers**

Martin White  
Managing Director  
Intranet Focus Ltd

Telephone: +44 (0) 1403 267030  
Online <http://www.intranetfocus.com/>  
Email: [contactus@intranetfocus.com](mailto:contactus@intranetfocus.com)

Revised April 2007

## **The Author: Martin White**

Martin White is Managing Director of Intranet Focus Ltd., which he established in 1999. Martin has written the Behind the Firewall column on intranet management issues for the US magazine EContent (<http://www.econtentmag.com>) since 2001, for which he is a Contributing Editor, a position he also holds for Intranets: Enterprise Strategies and Solutions (<http://www.intranetstoday.com>) and for which he is Reviews Editor. Martin was a workshop leader for Nielsen Norman User Experience events in 2005 and 2006, and is also taking part in the 2007 event.

Martin is the author of The Content Management Handbook, which was published by Facet Publishing Ltd in early 2005. His latest book, Making Search Work, was published in March 2007, also by Facet Publishing.

Martin was Chairman of the Online Information Conference (<http://www.online-information.co.uk>) from 1999-2006. In 2005 he was the recipient of the Information Industry Award for Lifetime Contribution. He has been Visiting Professor at the Department of Information Studies, University of Sheffield <http://www.shef.ac.uk/is> since 2002 and is a member of the Governing Board of CAB International. (<http://www.cabi.org>), acting as Chairman of the Finance and Audit Committee. He is also a member of the Publications Board of the Royal Society of Chemistry.

## **The Company: Intranet Focus Ltd**

### **Designing and enhancing intranets and extranets**

For organizations that have not yet set up an intranet we can carry out an information audit to confirm the information requirements needed to achieve the objectives of the organization, and from these develop a content strategy, information architecture and governance structure.

For organizations that have an intranet, or a number of departmental intranets, we can assess their design against current good practice, and undertake user surveys and usability tests. We can develop information architectures and metadata schemes. The business experience of our consultants enables us to support multi-national/multi-lingual intranets. We also provide guidance on the integration of intranets as the result of a merger or an acquisition.

### **Content Management and Search software selection**

We support the selection and deployment of content management software. We can develop a content management strategy, and from this prepare a formal RFP that can be sent out to a short list of vendors. To assist in the selection of a vendor we have developed a checklist based on our experience in major projects in North America and Europe. Once the vendor has been selected we can work with the client and the vendor to develop realistic implementation and content migration strategies. We can carry out similar projects for the selection of enterprise search software and corporate portal software. We maintain complete independence from any vendor.

## Introduction

This briefing paper outlines some of the areas where intranet managers need to ensure that they have not inadvertently breached legal and regulatory requirements, including issues arising from the increased use of electronic documents, and ensuring that intranets can be accessed by visually impaired users. The paper is written in the context of UK law, but should be broadly applicable to many other countries. Nothing in this paper should be taken as a legal opinion.

The paper covers

- Access by visually impaired staff
- Copyright
- Database rights
- Document and records management
- ISO9000 and quality management procedures
- Permission to publish
- Security and confidentiality
- Freedom of Information Act

Intranet Focus Ltd have also prepared a paper on the implications of the Data Protection Act on intranets which is available on <http://www.intranetfocus.com>

## 1. Access by visually impaired staff

Although the requirements of visually disabled users are now gradually being taken into account in designing web sites intranets, being home-grown, often ignore the basic principles of being able to be accessed by disabled users. The requirements of the UK Disability Discrimination Act must be taken into account in the design of intranets. Not only should the site be designed so that employees with limited or no vision can use the intranet, but also employees who may not have the motor skills to manipulate a mouse correctly over a complex set of images on a screen. The RNIB site [http://www.rnib.org.uk/xpedio/groups/public/documents/code/public\\_rnib008789.hcsp](http://www.rnib.org.uk/xpedio/groups/public/documents/code/public_rnib008789.hcsp) contains a wealth of useful guidance. In the USA there is now Section 508 of the Federal Code, and although this only applies to Federal websites the general principles are very similar to those in the UK. Two web resources are <http://section508.gov> and <http://usability.gov/accessibility/> The Usability.gov site lists many other web sites providing advice on accessibility issues.

If content management software is being used then it is important to ensure that the screens that contributors will be using to add or review content also conform to accessibility standards.

## 2. Copyright

Current copyright legislation does not distinguish between print and electronic copyright. On 22 May 2001 the first of what the European Commission regards as the Second Generation of copyright directives was adopted. This is the Directive on Copyright and Related Rights in the Information Society (2001/29/EC). This Directive has a much broader horizontal impact than the rather narrow Directives of the 1990s, with the aim of harmonising EU legislation as part of the continuing move towards a Single Market. The EU Member States have to bring their national legislation into line with the Directive within eighteen months, i.e. December 2002.

The reality is that there is far less harmonisation than the Commission sought to achieve. This is largely because of Article 5 of the Directive that sets out some of the exceptions to the

implementation of the Directive with the introduction "Member States may provide...." This gives considerable scope to national legislators to adopt whichever clauses they want, depending to a large extent on the lobbying that will no doubt be carried out in each country.

Another issue is raised by Article 6 which deals with electronic copyright and electronic rights management systems. These systems were not anticipated in the current national legislation in the EU, and therefore each country will almost certainly either have to pass new statutes or make very radical interpretations of existing legislation.

Electronic journal access through an intranet is the main area where compliance with copyright agreements is going to be important to impose and monitor. It is the secondary use of articles that needs to be managed with care. Usually the initial access is only permitted under strict conditions, but once the article is passed on, perhaps as an attachment to an email, then it may not be clear to the recipient that the article can not then be forwarded to others. It is important to ensure that everyone is aware of license agreements and that procedures are in place for monitoring compliance.

### **3. Database rights**

Associated with copyright are the provisions relating to database rights, where there is now a European Commission Directive.. This is a very complex area, but is very important in an intranet situation where it is easy for an individual or a group to compile a database on an intranet that may contain a mixture of documents and other material for which the institution holds copyright and also documents acquired from other institutions or information services. There may be infringement in the act of compiling the database, which is then compounded if the database is made available to others outside of the institution, perhaps to other members of a research team in another university or corporate laboratory.

### **4. Document and electronic records management**

In the rush to add documents to an intranet, and to make sure that they are published at the earliest possible opportunity, little attention may be paid to what happens to documents that are now out-of-date. This can be of particular importance with staff policy manuals. For the sake of an illustration take the hypothetical case of a laboratory safety manual that had been converted to intranet delivery. A laboratory technician is injured, and claims that there were no guidelines in the safety manual about what they should have done in that particular situation. The current version does have clear guidelines, but the accident happened a few months ago. If this case comes to a tribunal are you in a position to show what the content of the manual was on the day in question, whether or not the technician had access to it, and had in fact read it. The situation can become more complicated when the virtual handbook is updated in sections, and considerable care needs to be taken to ensure that all the individual sections cross-reference to each other correctly, and that all users are aware of what sections are new or revised.

Of paramount importance is that an effective method of version control is instituted for all documents placed on an intranet. The intranet is often used to facilitate group working but without using some of the more sophisticated document management software applications. Sometimes a document is posted on the intranet as a Word file, with the intention of tracking changes through the rather limited range of options available in Word. The result can then be that no-one is quite sure which version they are working on. At the very least the header and footer fields should be used to denote the version of the document, even if they are then deleted in the final document. One approach that is worth considering is to save final versions of documents in a pdf format. Although they can still be altered by anyone with the full Acrobat software suite, few members of staff are likely to have this available.

In the UK the lead on managing electronic records has been taken by the National Archives <http://www.nationalarchives.gov.uk/services/> . Although the standards that have been developed are targeted at public sector organisations they also represent best practice for other organisations. Another valuable resource is the Model Requirements for the Management of Electronic Records (MoReq), developed on behalf of the European Commission. <http://www.cornwell.co.uk/edrm/moreq.asp>. This is due to be updated in early 2008.

## 5. ISO 9000 and quality management policies

Although the ISO9000 series of standards is widely adopted as a quality management framework, all quality management policies usually rely on a formal review of documents, with the signature of the reviewer appended to the master copy of the document concerned. Moving these procedures into an intranet environment will not present any significant problems provided that care is taken to ensure that the revised procedures have been audited and approved. In the case of ISO 9000 this is carried out under the auspices of the British Standards Institution. Just creating a mirror-image of the existing manual procedures may not be adequate. One area that is sometimes overlooked is how easy it is for the independent auditor to conduct the audit. There may be similar procedures, for example in health and safety management, where the pragmatic intranet solution may not be admissible in a legal or regulatory review.

Looking at ISO9000 in another light, creating a quality management policy for an intranet can be a very worthwhile task, and this will be essential if the intranet plays an important role in procedures that are managed within ISO9000.

Permission to publish

One of the major problems with an intranet is getting people to publish documents on the intranet once the initial enthusiasm has been overtaken by the realisation of the effort involved. It is important not to let the quality management of the intranet become degraded. Clear guidelines on what is acceptable to be published, the procedures for assessing suitability, and the penalties for infringement need to be available to all users of the intranet. There is a danger in seeing the implementation of a content management system as a way to control content through the work-flow functions. This is not an appropriate use of work-flow. [http://www.cmswatch.com/Features/OpinionWatch/FeaturedOpinion/?feature\\_id=95](http://www.cmswatch.com/Features/OpinionWatch/FeaturedOpinion/?feature_id=95)

There is an ancillary problem here with e-mails. Because of the rather colloquial nature of e-mails the sender often forgets that they are sending an official document, just as if they wrote a letter. There have been a number of instances on various listservs where library staff have commented adversely on the service that they have had from subscription agents or library software suppliers. Circulating an e-mail with these comments is emphatically not the same as having a word with colleagues at a professional meeting. An email sent with a ac.uk or any other 'corporate' identifier in effect is a legal communication from the institution. The question should always be asked "Would the Managing Director be willing to countersign a letter containing these comments and going to the same circulation list?" Usually the answer will be "No!". The same applies to discussion lists.

## 6. Security and confidentiality

With the exception of personnel records and examination papers most people tend to make up document security policies as they go along. This may work (in theory) with paper documents, where the process of copying may be in itself a deterrent to wider circulation, but

that is certainly not the case with electronic documents. This is where an intranet can be an effective security mechanism. With e-mail the speed with which an attached file can leap around an organisation, or even outside an organisation, can be quite frightening, and tracking down just who started the chain of distribution can be very time consuming. If the email system is used to point to the document on the intranet, then the access logs on the intranet server can be used to identify who has downloaded a copy of the document. Moreover additional passwords and IP address filters can be introduced to ensure that there is some chance of controlling access to the document. Of course once downloaded the document can still be circulated by email or photocopier, but at least it may make people stop and think before circulating a document.

Another issue that need so be considered is the way in which documents are indexed, listed and identified by a search engine. There was one case I was involved with where an employee found the agenda to a meeting in which the subjects to be covered were set out in sufficient detail for an early warning of possible redundancies to circulate immediately around the organisation, even though the preparatory documents themselves were in a secure folder. The assistant preparing the agenda had not been made aware of the power of the search engine on the intranet! Even the circulation list of a document can give rise to a breach of confidentiality. Another way in which security can be breached is through the linking from one document to another.

Although in theory intranet servers can log all transactions, in practice care needs to be exercised in how these logs are used. This is especially the case where staff may be seeking information on job opportunities, or checking out grievance procedures. In these and other situations it could be very dangerous to jump to conclusions about the intent behind these actions, and there should be clear policy guidelines about the way in which access to an intranet is logged, the purposes to which the logs are put, and who sees the transaction logs. These need to be evolved in consultation with appropriate members of staff, or representative bodies, with any local issues being taken into account.

## **7. Freedom of Information Act**

The Freedom of Information Act 2001 came into force in England, Wales and Scotland on 1 January 2005 and there is a separate Act for Scotland which has similar provisions. Through the provisions of the Act members of the public have rights of access to a wide range of information from public sector organisations, much of which may be on the intranet. The implications of enquiries under the Act as regards access to this information need to be taken into account. In the UK the legislation is under the auspices of the Department for Constitutional Affairs <http://www.foi.gov.uk/> and the independent monitoring is the responsibility of the Information Commissioner <http://www.foi.gov.uk/>