Legal issues for intranet managers

Intranet Focus Ltd Research Note 05/12

May 2012

Intranet Focus Ltd
12 Allcard Close
Horsham RH12 5AJ, UK
+44 1403 267030
www.intranetfocus.com

Summary

It is important that intranet managers are aware of national legislation, regulations and guidelines that an intranet should be compliant with. Two of the most important areas are web accessibility and data privacy, but this Research Note also covers copyright, defamation, information security and records retention. This is not a complete list of relevant legislation. Companies working in the financial services sector will be subject to additional compliance requirements, and in many countries public sector organisations may be subject to Freedom of Information requests. The key maxim is that ignorance of the law is no defence. Intranet managers do not need to become lawyers but probably need to be as close to corporate legal staff as they do to the corporate IT staff.

Contents

Research Notes

This is the fifth in a series of Research Notes that Intranet Focus Ltd are publishing in 2012. For further information see http://www.intranetfocus.com/resources/downloads. Previous Research Notes covered enterprise mobile strategy development, enterprise search team management, digital workplaces and virtual teams.

1. Introduction

Intranet managers need to be conversant with a number of areas of law and regulation that apply to intranets. The commentary provided on these topics in this Research Note should be regarded as being for the purposes of illustration only, does not constitute a legal opinion and legal advice should be sought for the jurisdictions in which the intranet is operational.

2. Accessibility

The term 'accessibility' is often used to refer to the usability of the intranet, and the extent to which it provides access to information. There is another, and more restricted, definition which covers the extent to which employees with visual, physical or other disabilities can make use of the intranet. In general there are no specific national laws specifically about web accessibility but there are usually regulations that prohibit discrimination against disabled employees in the work place. One of the challenges is to understand the implications of these regulations on the design and functionality of the intranet.

The starting place for any intranet manager is the Web Accessibility Initiative of W3C, the World Wide Web Consortium. The key elements of the Web Content Accessibility Guidelines (WCAG) 2.0 are

Perceivable

- Provide text alternatives for non-text content.
- Provide captions and other alternatives for multimedia.
- Create content that can be presented in different ways, including by assistive technologies, without losing meaning.
- Make it easier for users to see and hear content.

Operable

- Make all functionality available from a keyboard.
- Give users enough time to read and use content.
- Do not use content that causes seizures.
- Help users navigate and find content.

Understandable

- Make text readable and understandable.
- Make content appear and operate in predictable ways.
- Help users avoid and correct mistakes.

Robust

- Maximize compatibility with current and future user tools.

As well as guidelines covering access to web pages the WAI has also developed Authoring Tool Accessibility Guidelines (ATAG) which are probably more important to typical distributed content authoring in an intranet than for the more centralised approach to content authoring for a web site.

However it is important not to see these guidelines as only being applicable to content pages on the intranet. With the growth of social media there could be barriers to employees who want to contribute to blogs, wikis and discussion groups but who cannot do so easily, if at all, with the current social media tools.

Also under development are guidelines for mobile accessibility and for media accessibility. The audio and video handling functionality of HTML5 needs to be considered with care so that accessibility issues are addressed from the outset. Another area that is often overlooked is the extent to which the user interfaces of enterprise search applications are compliant with the WAI guidelines. At present there is no work in progress on search interface accessibility but this may change before too long as search interfaces with filters and facets become ever more complex.

3. Copyright

Intranets perform a valuable role in acting as digital libraries of both internal and external content. External content will always be subject to copyright, which means for example that a section cannot be taken from a copyright work and used without a citation. It may be regarded that the intranet is only used by employees and so copyright does not apply as the organisation is not republishing the information. This is not a safe assumption to make, especially if suppliers, contractors and customers have access to some parts of the intranet or proposals and contract documents contain extracts from copyright information, such as standards.

The copyright of photographs is another area that intranet managers need to be aware of. An image may have been downloaded from Google or some other site, but the copyright of a photograph resides with the photographer, and cannot be used without their permission and possibly a fee. Photographs taken by employees may be covered by the contract of employment, but once they have left the company then the copyright returns to them. If an employee leaves the company and asks for all instances of their photographs to be destroyed the intranet manager needs to be able to track down all the photographs.

4. Data privacy

A substantial challenge with intranets is ensuring compliance with data privacy legislation, especially if the organisation is subject to EU legislation, which extends to anyone from any country that is working in the EU. The problems of conformance are not just related to intranets. The same issues apply to e-mails and any other form of transferring data, such as a flash drive, or in a lap-top computer being taken out of the country. For example, sending details of an employee's cv to the USA from the UK without consent could be in breach of the legislation. There is a view by some companies that if they only send information to other sites of their company then the legislation does not apply. This is not the case, and full consent needs to be obtained. This is because there is also a very important distinction between personal information and sensitive personal information in EU legislation.

Sensitive personal information covers

- the racial or ethnic origin of the data subject,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence

One of the key issues is that a person has to give their informed consent for this Sensitive Personal Information to be held in a database. Some intranets have an internal staff newsletter. In the interests of good communication there might be a news story about how a member of staff had been ill, but was now coming back to work for a few days a week. This could be regarded as sensitive personal data, as it

related to the health of the person, and this should not then be circulated electronically without the permission of the person concerned.

Many consulting projects, especially in human resources and change management, may require the consultants to check on personal information about employees. Using a corporate intranet from a single site to gain access to this information is likely to be forbidden, and of course if this information is to be held by a third party such as a consulting company, or an outplacement agency, then the employee's permission needs to be sought in advance. The employee also has the right to ensure that the information being held is correct, and this will require companies to implement intranet systems so that the employee can only see their own record, and not that of others. For employees that have left the company this right will extend as long as their file is maintained, which also gives rise to a range of problems, such as the time that a company should reasonably maintain that file.

A major issue with search log analysis, especially in the EU, is the data privacy issue. In reviewing intranet search logs there could be searches on voluntary redundancy, sexual harassment or discrimination or for the addresses of senior staff. All these might be taken as an indication that the person carrying out these searches was planning to take redundancy, sue the organisation for sexual harassment or discrimination, or send the addresses of senior managers to an animal rights activist group. The extent to which search logs might be construed to contain personal information has not yet been tested in the courts.

Data privacy compliance is especially important to take account of in the use of photographs on staff databases. Because a photograph will almost certainly contain information that enables a person's racial or ethnic identity to be inferred (even if incorrectly) staff photographs fall under the provisions of Sensitive Personal Information, and specific permission needs to be sought from each member of staff before their photograph is added. This has to be informed consent, so the member of staff needs to understand the implications and cannot be penalised for not giving consent. The fact that the photograph is on a staff badge does not mean that the photograph can be used for a staff directory. The photograph on a staff badge is there to enable security staff to ensure that the badge is being used by the designated badge holder.

On 25 January 2012 the European Commission published a proposal for a new regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data. There are some substantial changes proposed to data privacy legislation, in particular the move from a Directive to a Regulation as a means of gaining greater harmony over Member State data privacy implementation. The risks of non-compliance under the Draft Regulation are substantially greater than under the current legal framework and, for the most serious breaches, a national data privacy authority may impose a fine of up to a maximum of 2% of a company's annual worldwide turnover. The new regulatory regime will come into force in 2015/2016 but the work needs to start soon on identifying any potential areas of non-compliance.

It is essential that the advice of lawyers specialising in data privacy is obtained. It is likely that in-house legal teams will not have any substantial expertise in this complex area, especially when an intranet needs to be compliant with a number of different national legislations. Currently around 40 countries have some form of data privacy legislation.

5. Defamation, libel and corporate liability

As the current Leveson enquiry into phone hacking by News International illustrates, a small email can cause a great deal of damage. It still comes as a surprise to some people that emails, even personal ones, written on a corporate email application, are the property of the organisation, and may need to be

disclosed as evidence. This also holds for corporate mobile text messages, though the situation in the case of BYOD mobile devices is not at all clear. Also corporate property are blogs, emails and discussion forums. It is quite easy to forget when using social media channels that the messages are proprietary to the company. Sounding off about a competitor or the employee of a competitor is a very dangerous action to take. Just because it is inside the corporate firewall does not mean that it will not leak.

As more intranets move towards becoming digital workplaces and connect the organisation to customers and suppliers it is even more important to consider liability of the organisation should a defamatory blog or Yammer post turned up on the desktop of another organisation, including a newspaper.

6. Information security

All organisations process information that is sensitive or confidential. This information needs to be held securely and not disclosed to unauthorised personnel. Information is also required to be held in such a way that it is available in a timely manner and that it is protected against deliberate or inadvertent change. Over the last few years issues of information security have started to rise up the list of corporate risks. Much of the attention of IT managers and information security professionals has been on making sure that information generated by their organisation remains behind the firewall. IT Managers are well aware of the problems created by a wide range of IT hardware and software, ranging from wireless routers to high-capacity flash drives, and attempts by hackers to break in to databases containing confidential and business-critical information.

However far less attention has been paid to implementing procedures to ensure that confidential information in documents remains suitably secure. In many organisations there is still little guidance for staff about how documents containing confidential information should be managed, or even a clear definition of what constitutes 'confidential information'. The extent to which information is confidential may change over time, and with the role of the employee in the organisation. Heavy reliance is probably being placed on email circulation lists to restrict documents to named individuals, but often there is no consistency of labelling on documents about the associated level of security, or at best this is only on the cover page, and not on the individual pages of a document or spread sheet. Taking off a watermark on an MS Office document is as easy as adding it in the first place.

Given the number of documents on any server the chances of a member of staff finding confidential information is probably very remote if all they are doing is working through a folder structure or listing documents by title. The challenge comes when a search application is implemented. As the search application builds the indexes if there is no way that the circulation and security permissions related to a document can be identified by the indexing engine then the document becomes, inadvertently, open access. Whatever search engine being used it can be instructive to just do a search for [confidential] and look through the results. It could well be that many of the results are to guidance notes on how confidential information should be managed, but can you be certain that this is the case for all the documents listed? Even just one might contain information that, if widely circulated by a disaffected member of staff, or more likely a temporary worker, could impact the operations and reputation the organisation, then that is one document too many.

7. Records retention policy

A "record" is evidence of an activity or decision and demonstrates accountability. It is not possible to define a record in terms of a particular category of documents, or by the age of the item. A comment in a blog or on a wiki could indicate that an action has taken place, and so becomes a record of that event taking place. The use of social media in this example is quite deliberate; in the world of records

management there is no such thing as formal and informal content. There is also the concept of a 'controlled document' but this refers to a document in which the revision history is important and that employees need to be aware of which version (not always the latest version) they should be using.

It is also important to distinguish between 'records' and 'archives'. A record has a limited and defined life-time, which may be seven years for financial returns to five years after a product has been withdrawn from the market. An archive is a collection of records that have a long-term, and often indeterminate life. All too often the terms 'record' and 'archive' are used as synonyms, which is not the case.

The issue about the extent to which information that is available on an intranet needs to be regarded as a corporate record is often overlooked because of a concern about the sheer volume of the content and the file formats involved. Often a document management system is in use as a way of managing corporate records, but such a system will rarely be used for the entire intranet, collaboration spaces and social media messages.

Increasingly videos are used to illustrate the way in which particular activities should be carried out. An example might be the way for an employee in the warehouse to use a forklift truck to load a vehicle. In due course the video might be updated, and the previous version deleted so that the 'correct' version is available on the intranet. But suppose that it was some years later that the warehouse employee suffered from a back ailment that they claimed was caused by inadequate information being presented in the video. When the organisation comes to defend itself can the video be found? An inability to locate the video might be used by the prosecution as evidence that the information was inadequate and that is why the video was deleted.

The situation is especially important to manage in the USA where Federal e-discovery rules can bring an intranet centre-stage in any legislative action. Where an organisation does not have a records manager then advice from a records management consultant working with the organisation's legal and risk managers is essential.

8. Summary

This Research Note has covered just six areas where intranet managers need to ensure that the intranet is compliant with relevant law and regulations. In most countries there will be other legislation that has to be taken into consideration. Examples would be Freedom of Information legislation and regulations affecting information access and distribution on companies providing financial services.

The key maxim is that ignorance of the law is no defence. Intranet managers do not need to become lawyers but probably need to be as close to corporate legal staff as they do to the corporate IT staff. In a few years infringement of the EU data privacy legislation could result in the organisation paying a fine of up to 2% of its turnover. The cost of legal advice at this time would be substantially less.

9. Checklist

The checklist below sets out the main actions that should be taken to ensure that an intranet is compliant with national legislation and industry guidelines.

Because of the implications of failure to comply any score of less than 13 Yes answers is a Fail

Current situation	**Yes/No**
We know the countries in which employees and contractors are using the intranet	
For each country we know the legal and regulatory requirements that are relevant to the intranet	
For each country with data privacy legislation we have a good working relationship with the manager responsible for compliance	
For each country an audit has been carried out by suitably qualified people on the extent to which the intranet meets these requirements	
Where there is any gap between the requirements and compliance a programme has been put in place to remedy the situation	
We monitor changes in national legislation and are ready to take appropriate action	
The intranet contains guidelines and standards on legal compliance issues, which have been signed off by managers at an appropriate level in the organisation	
Content authors, including those using social media, have to sign a document that confirms that they have read and understood the implications of the guidelines and standards	
Content authors are trained in how to contribute content that is fully compliant with guidelines and standards	
These guidelines and standards are brought to the attention of new employees at the earliest opportunity	
We ensure that we are compliant with the guidelines of the WAI, and are monitoring the development of new guidelines in the areas of mobile and media content deliver	
We have assessed our search applications as being accessible for employees with visual and other disabilities	
Employees with visual and other disabilities are involved in the evaluation and implementation of new features on the intranet	

Resources

Accessibility

Web Accessibility. Jenny Craven (editor). Facet Publishing, 2008. http://www.facetpublishing.co.uk

Web Accessibility in Mind
http://webaim.org/

Royal National Institute for Blind People
http://www.rnib.org.uk/professionals/webaccessibility/usefullinks/Pages/useful_links.aspx

W3C Web Accessibility Initiative (WAI)
http://www.w3.org/WAI/

Data privacy

Baker and McKenzie's Global Privacy Handbook 2012 http://www.bakermckenzie.com

EU Protection of Personal Data
http://ec.europa.eu/justice/policies/privacy/index_en.htm

EU National Data Commissioners
http://ec.europa.eu/justice/policies/privacy/nationalcomm/index_en.htm

Privacy Laws and Business
http://www.privacylaws.com/

Summary of UK legislation with implications for intranets
http://intranetizen.com/2011/05/10/10-laws-for-intranet-managers/