ACT NOW TRAINING

May 2011
Information Law
Newsletter

ALL CHANGE FOR ISEB

The Information Systems Examinations Board (ISEB) (part of the British Computer Society) has revised the syllabus for its popular courses leading to the internationally recognised qualifications in Freedom of Information and Data Protection. The changes make the qualifications more relevant to practitioners and those who wish to quickly get up to speed with information governance legislation.

Act Now is one of the UK's leading providers of ISEB courses. The courses are designed in such a way as to allow even those with a basic knowledge of DP and FOI to benefit and take the exam. Both courses are also accredited by the Solicitors Regulation Authority and the Institute of Legal Executives for CPD Credits.

	FOI	DP	OVERALL
ACT NOW TRAINING	92%	80%	85%
OTHER PROVIDERS	68%	73%	72%

LIVE WEBINARS

Training Without the Strain of the Train

Act Now continues to push the boundaries of training delivery in information law and governance. Over the past few months we have delivered a number of live online courses. No struggling on trains, less time away from the office and more cost effective than face to face training, our online courses are proving a big hit with delegates

www.actnow.org.uk/content/91

All courses are live and fully interactive (not mere recordings). Our experienced trainers take delegates through their presentation just as though you were sitting in front of them. Delegates see the presentation, as well as any other documents the trainers use, on their screen in real time. Delegates can listen and ask questions at any time by phone, through their computer's microphone or by instant messaging. Delegates can download paper copies of the slides and other relevant materials. At the end of the course there is usually a quiz to complete.

All our online courses are accredited by the Solicitors Regulation Authority and the Institute of Legal Executives for CPD Credits. Delegates can download a certificate of attendance after the event. Forthcoming Courses include:

- Protection of Freedoms Bill
- Cloud Computing and Data Protection
- Copyright Law
- FOI: An Introduction
- FOI: An Update
- EIR: An Introduction
- DPA: An Introduction
- Handling Subject Access Requests
- Cookie Law: EU Privacy and Electronic Communications Directive
- FOI and Datasets

Many of these courses are free. Others carry a small charge (from £10 plus vat).

Full details:

www.actnow.org.uk/content/83

Revised ISEB Courses

MORE QUALITY
MORE TUTOR HELP
REDUCED FEES

The changes to the ISEB syllabus have prompted us to revise our course delivery to make it even easier for our delegates to pass the exam.

We now include:
A full three hour mock exam which is tutor marked
Live webinars to aid delegate study and revision
A competitive fee; now reduced by £200

STOP PRESS
STOP PRESS
STOP PRESS
STOP PRESS

REDUCED FEE
£1750 + vat
In the current economic climate we have slashed the delegate fee on all our ISEB courses by £200 plus vat.

This fee includes all course materials, lunch, the exam fee and no hidden extras.

Our next ISEB courses start in Edinburgh and Manchester in the Autumn

We still have a few places left :

www.actnow.org.uk/content/29

In this issue:

And much more...
Previous issues are archived on our website.
This newsletter contains links to other websites. We cannot be responsible for content or availability of other sites. Please read the notice on page 19.

Next issue:
September 2011

Freedom of Information

Datasets: The New Law

In January the Government announced plans to amend the Freedom of Information Act 2000(FOI) to ensure public authorities proactively release data in a way that allows businesses, non-profit organisations and others to re-use it for social and commercial purposes. Clause 92 of the Protection of Freedoms Bill, currently going through Parliament, contains proposals to require all public authorities to release datasets in a re usable electronic format. If passed, which seems very likely, it will mean more FOI requests from commercial companies and data aggregators and fewer reasons for public authorities to say no.

What is a Dataset?

A dataset is a collection of information held in electronic form where all or most of the information meets the four criteria set out in the following paragraphs (of the new section 11(5) of FOI):

• It has to have been obtained or recorded for the purpose of providing a public authority with information in connection with the provision of a service by the authority or the carrying out of any other function of the authority

• It is factual information which:

(a) is not the product of interpretation or analysis other than calculation, in other words that it is the 'raw' or 'source' data; and

(b) is not an official statistic the meaning given by the Statistics and Registration Service Act 2007 ("SRSA 2007"). (Official statistics have been excluded from the definition of datasets as the production and publication of official statistics is provided for separately in the SRSA 2007.)

• It remains presented in a way that (except for the purpose of forming part of the collection) has not been organised, adapted or otherwise materially altered since it was obtained or recorded. (Datasets which have had 'value' added to them or which have been materially altered, for example in the form of analysis, representation or application of other expertise, would not fall within the definition.)

Examples of the types of datasets which meet the definition include postcodes and references used to identify properties, spend data, lists of assets and information about job roles in a public authority.

Re Usable Electronic Form

Clause 92 of the Bill will amend section 11 of FOI (means by which communication to be made). At present section 11 allows a requestor to choose the format of the information to be supplied to him. As long as this is reasonably practicable the public authority must give effect to his preference.

A new section 11(1A) will mean that in future where a request is made for information held by a public authority that is a dataset, or which forms part of a dataset, and the applicant requests that information be communicated in an electronic form, then the public authority must, so far as is reasonably practicable, provide the information in an electronic form that is capable of re-use. This is in a machine-readable form using open standards which enables its re-use and manipulation. Thus, in future, authorities will be prevented from turning an Excel spreadsheet into a PDF document before releasing it in order to stop recipients conducting their own analysis or re formatting the data.

New section 11(1A) uses the words "so far as is reasonably practicable". There is no absolute duty for datasets to be provided in a re-useable format as it is recognised that, in some instances, there may be practical difficulties in relation to costs and IT to convert the format of the information.

Copyright Works

New section 11A(2) provides that when communicating a dataset to an FOI applicant

Continued on page 3

Freedom of Information

Datasets: The New Law

Continued from page 2

and all or part of the dataset contains a relevant copyright work, a public authority must make the copyright work available for re-use in accordance with the terms of the specified license. The terms of such a license will be specified in a new section 45 Code of Practice. It is not known at present whether such licenses will allow public authorities to charge for allowing re use.

The definition of a "relevant copyright work" includes a copyright work (as defined by the Copyright Designs and Patents Act 1998) as well as a database subject to a database right. This provision is designed to prevent public authorities from refusing to release datasets on the basis that they contain a copyright work and so are exempt under section 43 (commercial interests).

New section 11A(1) provides for the four criteria which must be met for the new requirement to allow re use of datasets (in section 11A(2)) to apply:

(a) a person must have made a request for a dataset or part of it

(b) the dataset requested includes a 'relevant copyright work'

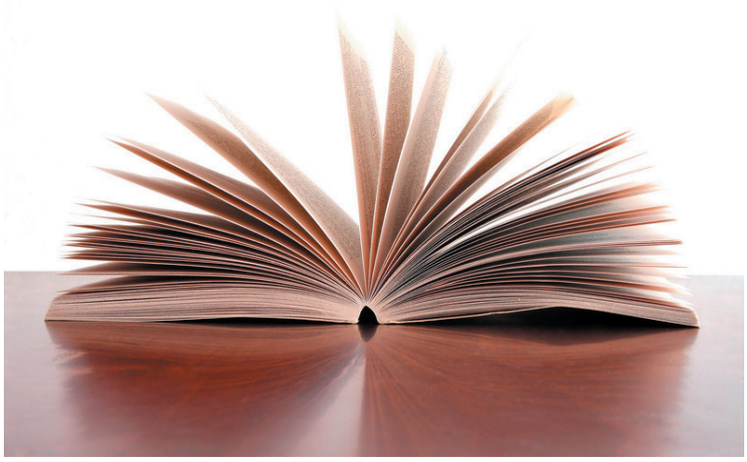
(c) that the public authority is the only owner of the 'relevant copyright work' (in other words that it is not owned in whole or in part by a third party); and

(d) that the public authority is communicating the relevant copyright work to the requester under the FOI (in other words it is not being withheld under one of the exemptions).

These provisions will require public authority information professionals and lawyers to brush up on their knowledge of copyright and database law. There are many cross references to the Copyright Designs and Patents Act 1998 as well as the Copyright and Rights in Databases Regulations 1997.

Proactive Publication

Once a dataset is disclosed following an FOI request, the Protection of Freedoms Bill amends FOI to place obligations on the public authority to make that dataset more widely available.



Under new section 19(2A) of FOI, Publication Schemes must include a requirement for the public authority to publish any dataset it holds, which is requested by an applicant, and any updated version of the dataset. All datasets published in this way will have to, where reasonably practicable, be in an electronic form which is capable of re-use and any relevant copyright work within it will have to be made available for re-use in accordance with the terms of the specified licence (as above).

New section 19(2A), requires authorities to publish any dataset as discussed above unless "the authority is satisfied that it is not appropriate for the dataset to be published". The Campaign for Freedom of Information (www.cfoi.org.uk), in its submission to the Protection of Freedoms Bill Committee on clause 92 of the Bill, has criticised this carve out as not within the sprit of the Act and because it involves a subjective element which will be difficult for the Information Commissioner to oversee. It remains to be seen whether this provision is amended as per the Campaign's suggestion to a "reasonably practicable" test.

Clause 92(5)(a) of the Bill amends section 45 of the FOI (issue of code of practice) to insert a new requirement for the code of practice to include provision relating to the disclosure by public authorities of datasets held by them. Paragraph (b) of the same clause sets out the different provisions relating to the re-use and disclosure of datasets that may, in particular, be included in the code. Paragraph (c) amends section 45(3) of the FOI so as to provide for the possibility of making more than one code of practice under section 45, each of which makes different provision for different public authorities.

The new FOI obligations to be introduced by the Protection of Freedoms Bill will no doubt mean more work for public authorities at a time when money is scarce and staff levels are being reduced.

There will be at least one new code of practice to implement as well as a new publication scheme to adopt. It will be interesting to see the terms of the "specified license" and to what extent, if at all public authorities, will be able to charge for allowing re use of datasets.

Freedom of Information

Being Open to Open Data- A Practitioner's Perspective

FOI Man

So you're an FOI Officer or Information Governance type in the public sector. You've been dealing with FOI requests for years now. You know your stuff. You listen to Act Now's podcasts, you've been on their training courses, you've maybe got an ISEB. Colleagues have just about got used to the idea that when you ask them for information to answer a request they should provide it within twenty working days. Even the Chief Executive has stopped complaining about having to disclose his expenses.

It's tempting to think you can slip into Auto-Pilot, or at least focus all your resources on trying to avoid data breaches and improving your records management (good luck with that). But no, along comes the Coalition Government and puts forward amendments to the Freedom of Information Act. The Protection of Freedoms Bill, currently progressing through Parliament, includes amendments which will require public authorities to disclose requested datasets in a re-usable format where practicable, to publish these disclosed datasets (the first time effectively that Disclosure Logs will have the force of law behind them, if only for a subset of FOI requests), and to pro-actively publish datasets as part of our Publication Schemes. We will even be obliged to allow re-use under conditions to be specified in the Section 45 Code of Practice.

This isn't coming out of nowhere. The Guardian Newspaper has been pushing for an open data policy from Government for years now with some success before, and especially since the election. Francis Maude gave a speech back in October at the Conservative Party Conference explaining the thinking behind the plans for dataset disclosures:

"Thousands of commercial and social entrepreneurs have been frustrated by their inability to obtain and reuse datasets. I'm sorry to say that some councils spend time and money deliberately making data unusable to anyone else."

Whether you agree with his comments or not, the game is changing. We need to get to grips with these new requirements sooner rather than later. The Protection of Freedoms Bill may well take some time to become law, but expectations have been raised.

So what are these datasets? On page 3 Ibrahim Hasan has discussed the definition set out in the Bill.

In practice, datasets are your raw data. In many cases their content will already be on your website or in your publication scheme. But they may well not be easy for others to use in their present form.

For example, there may be contact details for different departments in your authority spread throughout your website. But if someone wanted to create a smartphone app that directed users to the right department at your authority, they would want all of that contact data consolidated into one spreadsheet that they can then easily manipulate and put together with other data.

It's not just the publication of these datasets that is important if you want to get ahead in Open Data. It's the licensing of re-use. Like me, you probably became a little disillusioned about the Re-use of Public Sector Information Regulations which came into force back in 2005. Without leadership from Government, it was difficult to make much progress with their implementation. But we now have that leadership and more importantly a ready-made licence to govern re-use of our organisation's data. The National Archives' Open Government Licence (OGL) is being promoted for this purpose. If your authority adopts it, you'll be allowing re-use of the data that you apply it to by anyone who wants to, as long as they acknowledge the source. If you find that the OGL doesn't suit your purposes, there will undoubtedly be other similar licences made available for use across the public sector in due course.

Many public sector bodies have made significant progress already. As well as the Government Datastore at data.gov.uk, public sector bodies have started to form consortia to establish regional datastores, such as those of London and Greater Manchester. Local authorities like Wigan and Camden have pages or even whole websites dedicated to publishing datasets. The Open University and the University of Southampton have pioneered the publication of open data in higher education.

What's slightly alarming is that the work on this so far seems to be bypassing FOI Officers. This shouldn't be happening – we've built up a vast knowledge of the information and data held by our organisations. We know, more or less, what data can be disclosed without concern. We even have an existing infrastructure – our Publication Schemes – through which we can make the datasets available. We should have an established role as the champions of openness and transparency within our own authority. But most open data projects seem to be led by others.

So my plea to fellow FOI Officers is this. If your organisation already has an Open Data project, get involved. Make sure your voice is heard. At the very least ensure that the Open Data pages on your website link to your Publication Scheme and vice versa. If your authority has not yet made moves in this direction, use the Protection of Freedoms Bill as an opportunity. Lead from the front. Make the case to your management. Obtain approval to use the OGL. Get those datasets online.

FOI Man is an FOI Officer in a public authority with several years' experience of implementing FOI procedures and answering requests. He writes a blog at www.foiman.com Follow him on Twitter (@FoIManUK) for his views on the latest FOI developments.

Freedom of Information

Re-use and Copyright

Regulations were introduced in 2005 to implement EU Directive 2003/98/EC on the re-use of public sector information. The Directive provides a number of minimum requirements that Member States must implement in order to ensure fair, proportionate and non-discriminatory conditions for re-use. The scope of the Directive and the subsequent UK legislation is narrow: the definition of a public sector body, for example, specifically excludes public sector broadcasters and their subsidiaries, and educational, cultural and research establishments, including "organisations established for the transfer of research results".

In addition, the regulations only apply to a document which has been identified by the public sector body as available for re-use, or has been provided to the applicant, or is accessible by means other than the making of a Freedom of Information (FOI) request. Finally, the regulations do not apply to any document in which a third party owns relevant intellectual property rights, and a public sector body would not be required to release a document which had been commissioned by them. A reasonable charge may be made by the public sector body for the re-use of information.

Recently, the introduction of an Open Government Licence (OGL) has simplified the process for re-use of public sector information which has been made publicly available. The licence allows for commercial and non-commercial exploitation and is reasonably unrestrictive in its application, allowing copying, publishing and adaptation of the information. However, not all published documents fall under this licence, as the OGL is an optional licence which public sector bodies can adopt if they so wish. It follows that information received by an applicant under FOI is also not automatically released under the OGL, meaning permission has to be sought before further use may be made of it.

The fact that legislation for the re-use of public sector information was introduced highlights a fundamental difference between access to information and subsequent use made of that information. Most instances of re-use involve the reproduction of information belonging to a public sector body, and as such come under the provisions of a different law: that of copyright. Clause 22 of the EU Directive on the re-use of public sector information clearly states that the existence and ownership of copyright and related rights (including database rights) in documents are not affected by the provisions of the Directive, and public sector bodies are not restricted from exercising their rights under copyright beyond the boundaries set by the Directive. In other words, public sector bodies may choose to licence their published material for re-use, but are not obliged to.

Increasingly, decision notices from the Information Commissioner's Office (ICO) contain concerns about copyright law. Copyright formed the crux of the argument in the House of Commons Decision Notice in 2010. The public authority claimed that it could not disclose the information requested because the email address to which it would be sent would infringe its copyright by automatically publishing the information on the website. The Information Commissioner found that responding to a valid address in compliance with the FOI Act is not an infringement of the Copyright, Designs and Patents Act (CDPA) in accordance with section 50. However, the Information Commissioner made it clear that subsequent and automatic publication of information can be addressed separately as a copyright rather than an FOI issue. The findings in the University of Central Lancashire Decision Notice strengthen the dichotomy between access (FOI) and subsequent re-use (Copyright): clause 96 states that "information which may be subject to disclosure under the [FOI] Act may also be subject to copyright protection", and that the public authority "is entitled to make the applicant aware that information is copyright protected and is able to protect its intellectual property".

The legislative framework and the ICO both recognise that copyright is a pertinent issue when dealing with subsequent re-use of material received under FOI and that it must be dealt with separate to the provisions laid out in the FOI Act. Copyright applies to works (literary, artistic, musical, films, sound recordings, broadcasts, typographical, databases) which are original expressions of an idea, but does not protect the idea itself and does not extend to protecting facts, numbers or names. Copyright holders have a number of exclusive rights, which include copying the work, issuing the work to the public (also known as the distribution right), adapting the work, and communicating the work to the public (such as publishing on the internet). Copyright in a work generally lasts for 70 years following the death of the author, but works created by the UK government are covered by Crown or Parliamentary (specific to works created or created under the direction of the House of Lords or House of Commons) copyright; the duration of copyright in those works is 125 years and 50 years respectively.

Defences to copyright infringement (or ways in which material can be used without infringing copyright) are listed in the CDPA; these include fair dealing for non-commercial research and private study, criticism and review, and for the purposes of news reporting (with the specific exclusion of photographs) as long as there is sufficient acknowledgment of the copyright holder. 'Fair' is not defined but is better explained as the use of an insubstantial part of the work. A rare possible defence to copyright infringement is the 'public interest' defence and is built on the provision in section 171(3) in the CDPA. Although relatively untested, this defence has cropped up in case law with mixed results. The defence has been successfully argued in cases where the public could directly suffer if the material was not published, yet only as long as no other defence applied and that it was necessary to reproduce the material exactly. The Court of Appeal upheld that a court would be entitled to refuse to enforce copyright of the work if the work is immoral, scandalous or contrary to family life; injurious to public life, public health and safety and administration of justice; or incites or encourages others to act in a way referred to in the first point . The scope of the public interest defence is very narrow; the act of reproducing copyright material and claiming the right to freedom of expression would not apply as part of the public interest test.

Finally, the Protection of Freedoms Bill currently progressing through Parliament is seeking to amend FOI legislation to allow for the disclosure and re-use of information (including datasets).

See Ibrahim Hasan's article on page 3

Emily Goodhand is a Copyright & Compliance Officer in the University sector. She has an excellent blog on copyright issues www.copyright4education.blogspot.com/
Please follow her on Twitter (@copyrightgirl)

Introduction to Copyright Webinar: Emily will be presenting a live webinar on this topic for Act Now Training : **www.actnow.org.uk/content/83**

Freedom of Information

Personal Data - Caselaw Roundup

In the past few months information about senior public sector employees, especially when leaving employment, has come under the FOI spotlight. There is no hard and fast rule about disclosing information about former senior employees; whether in the form of compromise agreements or voluntary redundancies. The key question is would disclosure be fair to the data subject? The answer depends on many factors including the circumstances surrounding the individual's departure.

Compromise Agreements

In February , the Tribunal (in Gibson v IC and Craven District Council (EA/2010/0095), http://bit.ly/jaWRug, ordered disclosure of information in a compromise agreement with the former chief executive insofar as it related to the use of public funds i.e. the precise financial settlement. The remainder of the information, more personal information from personnel files, could be withheld on the basis of the section 40 exemption (e.g. tax codes and pensions contributions).

The Tribunal found that all information in the requested compromise agreement was personal data. It agreed that generally information on compromise agreements should not be disclosed – but, as ever, context is important. Here the case concerned a very senior employee (the chief executive) who left office with the Council finances "in disarray", but the auditor had – ultimately – approved the settlement paid under the compromise agreement.

As to the lawfulness of disclosure, it observed that this term is not defined in the DPA, but "seems to mean that information may not be processed when the law does not allow it, as opposed to when two parties have entered into a voluntary agreement not to disclose the information". In other words, a mere contractual agreement as to confidentiality does not suffice to render disclosure "unlawful".

As to the fairness of disclosure, the Tribunal distinguished between information on the use of public funds and other information. It noted that compromise agreements are "personnel matters", generally attracting a strong expectation of privacy. Although "personnel" information comes into existence as part of the employee's professional (rather than personal) activities, some of it (such as pension contributions and tax arrangements) are "nevertheless inherently private and would attract a very strong expectation of privacy and protection from the public gaze".

Again, expectations of confidentiality were not decisive on the question of fairness: the Tribunal did "not regard it as reasonable for the ex-CEO (or the council) to expect that certain information relating to the use of public funds, to be hidden from public gaze by virtue of a confidentiality clause agreed between them". Nor was the Tribunal impressed by submissions that disclosure would have a substantial adverse impact on the ex-CEO's employment prospects or personal life. Ultimately, fairness and condition 6 from Schedule 2 DPA were determined in similar terms: the Tribunal found that "the legitimate interests of members of the public [in transparency] outweigh the prejudice to the rights, freedoms or legitimate interests of the ex-CEO only to the extent that the information concerns the use of public funds".

The Tribunal gave weight to the existence of an agreement between the college and Mr Gates which included a provision at Clause 15 that expressly limited the amount of information that would be made available to the public about the termination of his employment. It felt that even in the public sector, compromise agreements may be expected to be accorded a degree of privacy as long as there was no evidence of wrongdoing or criminal activity present.

Bonus Information

The Tribunal decision in Davis v IC and Olympic Delivery Authority(EA/2010/0024), http://bit.ly/iuq8qK, concerned a request for bonus payments, performance targets and the targets levels achieved in relation to senior staff at the ODA. In coming to its decision, the Tribunal distinguished between bonus information and performance assessment information.

It ordered disclosure of certain information relating to the bonuses of senior employees of the ODA: the maximum performance-related bonuses to which the chief executive and communications director were contractually entitled, and the percentage of the maximum available bonus actually paid to certain other members of senior management.

The Tribunal did not think that disclosure of this information involves an unwarranted interference with their rights and freedoms. It noted that a certain amount of information about the comparative success against targets may be gleaned from the information that has already been published and it believed that those taking on such high profile and well remunerated positions on a project of such justified public interest should expect greater than normal publicity about their role and pay. The individual executives in this case may be expected to have been aware of the general trend of openness and transparency in the public sector and of its likely impact on the positions they have attained.

The Tribunal decided, however, that details of the performance targets which individuals failed to hit to 100% satisfaction should not be disclosed. It said that in each case disclosure would involve an intrusion into an element of the individuals' lives which, while work-related, has such a direct impact on career progression and personal self-esteem that it would only be warranted if, in addition to the matters of public interest identified, the operation of the remuneration scheme justified significant criticism.

Names of Staff

Where there is a risk to staff safety if there names are disclosed, a public authority will be right to err on the side of caution. In Wild v IC and Chief Constable of Hampshire Constabulary (EA/2010/0132) the Appellant requested from the Chief Constable dates of pre-hunt meetings in the last five years and the names of police officers attending pre-hunt meetings with organizers of the Isle of Wight Hunt. The Police responded, providing dates, but refusing to disclose the names of the officers in attendance. The Commissioner considered the section 40(2) exemption as clearly the names were third party personal data. He concluded that the disclosure would result in a breach of the first Data Protection principle that data should be processed fairly and lawfully. He accepted that the disclosure may lead to the harassment of the officers identified and consequently the disclosure would be unfair to those officers. The Tribunal upheld the Commissioner's decision.

Freedom of Information

News in Brief

The Perils of Redacting

A report (**http://bit.ly/hbsCnS**) in the Daily Telegraph on April 18 confirmed an issue that Act Now's FOI trainers have heard plentiful horror stories about. Several government departments including the Ministry of Defence, the Department of Health and the Department for Communities and Local Government have been caught out by a relatively simple mistake.

Redacted documents made available under FOI and either disclosed or published often allow information to be easily obtained. The commonly used technique of applying black blocks of text to a Word or similar program and then turning the document into a PDF often does not work. If you select and copy the text of the completed document and paste it into Word etc., you will see the full document, not the redacted version.

The Telegraph reports a range of sensitive issues – including information about nuclear submarine security – being accidentally available as a result. A review is currently underway to see how far the problem goes.

Our advice to avoid this problem is as follows:

• If you are using the PDF method, remove the text completely from the original document, and replace it with a black block or similar item

• Alternatively, turn the redacted document into a picture (e.g. a GIF or JPEG, which is a picture of the original rather than a PDF version of it

• Print the document, mask the redacted information with post-it notes or a thick black marker pen, and then scan it in. Look at the final version if using marker pen, as leaving text visible under the marker has caught out some organisations!

• Buy software designed specifically to prevent access to the redacted data – this is a potentially expensive option, and only appropriate to organisations who regularly have to send out redacted documents

• Print an appropriately edited version, and post it out!

• MOST IMPORTANTLY, check the document before you send it – if you are legitimately withholding something, make sure with every document that you are only giving out what you intend to give out.

Publicly Owned Companies

The definition of a "publicly-owned company" under section 6 FOIA is being amended by the Bill. Section 6(1) will no longer apply only to bodies wholly owned by a FOIA-listed authority, but also to those wholly owned by "the wider public sector". Section 6(2) is adjusted so that it also pivots around the concept of "the wider public sector". The effect of this amendment is that even a publically owned company –owned by more than one public sector organisation will be subject to the Act.

Draft Local Government Code

Following Eric Pickles' muscular debut as Secretary of State for Communities and Local Government, savaging high pay in local government and demanding that all spending above £500 is published, the Government has come forward with more concrete proposals. The 'Code of recommended practice for local authorities on data transparency' is in draft and out for consultation: **http://bit.ly/fOfb4A** The consultation ended on 14 March 2011. Read Tim Turner's article:
www.actnow.org.uk/content/45

Early Retirement Package

In Pycroft v IC and Stroud District Council (EA/2010/0165), **http://bit.ly/m6Afx9** The Appellant wanted to know the package that was offered to the Director of Housing when he took early retirement. The context of the request was an auditor's report which observed that the councils former Director "did not ensure that staff had taken ownership of managing the budgets" and there was an overspend on the Housing Revenue Account for which he was ultimately responsible.

In considering fairness under section 40(2), the Tribunal noted that the pension package is calculated by reference to the sum of past service and not performance. It is just not a snapshot in time of a person's financial situation, disclosure of which would be more likely to be fair especially if the person has just ceased employment in the public sector and so has benefitted from public money. Disclosure of a retirement package today would (if e.g. index linked) enable that person's income to be calculated for the rest of their life, long after they had ceased to be accountable to the public.

The Tribunal agreed with the Commissioner that disclosure of this information would not be fair, The disputed information goes beyond information directly concerning the individual's public role or decision making process and relates to personal finances. Although it is related to the individual's employment (in the sense that it is payment for service), it is not information so directly connected with their public role that its disclosure would automatically be fair.

The Tribunal also observed that in light of the Strategic Director's seniority and the problems with the HRA overspend this would have been a high profile retirement and that sufficient information was already in the public domain to enable the propriety and timing of such a retirement to be debated in any event without disclosure of the terms.

This decision should be noted by those dealing with requests for information about retirement packages to allegedly poorly performing public sector employees. It shows that just because they have received public money, does not mean disclosure of their information is automatically fair.

MOJ Annual FOI Stats

The Ministry of Justice has published the annual FOI statistics for central government in 2010. The report is available from **http://bit.ly/iWobYx**. The Excel tables can be downloaded from **http://bit.ly/l3tVsM.**

FOI Podcast No 25

Ibrahim Hasan's latest FOI podcast has now been published. It covers major decisions of the Information Commissioner and the Tribunal in December to February 2011. You can also read the script for the previous podcast. Listen, learn and claim ½ a CPD credit for free:
www.actnow.org.uk/content/21

FOI Update Workshops

A full workshop examining the latest FOI decisions of the Commissioner and the Tribunal will be held in 2011 in London, Manchester, Bristol , Belfast.

Environmental Information Regulations

The Cinderella Regime?

When Christopher Graham, Information Commissioner, in a press statement in December last year accompanying an undertaking signed by the University of East Anglia (UEA), said "This is the first occasion on which we have sought formal undertakings to secure compliance with the Freedom of Information Act" few media commentators noted that the UEA's identified failings had in fact been in responding to requests for environmental information, and, that, accordingly, it was in fact the Environmental Information Regulations 2004 (EIR) which had been breached.

This apparent sidelining of the EIR is certainly not without precedent. In 2009 the Scottish Court of Session considered the important issue of whether there exists a right to documents, as well as information, under the Freedom of Information (Scotland) Act 2002 (Glasgow City Council and Dundee City Council v Scottish Information Commissioner [2009] CSIH 73). Nothing in the court's judgment, however, indicates that any of the parties considered whether information about registers of private water supplies and registers of roads was likely to be environmental information, and that requests for such information should have been handled under the Environmental Information (Scotland) Regulations 2004. Additionally, a considerable number of Decisions Notices by the IC appear to have been issued under FOIA, when they rightly should have been under EIR (by example I give you, following an exhaustive two-minute trawl of the archives, FS50176919 on water meters and water wastage, FS50078602 on street development contracts and FS50094592 on fisheries' harvests). When even the regulators and the judiciary overlook them it is difficult to avoid the conclusion that the EIR are the Cinderella regime among the access to information laws (although it might be a bit unfair to call FOIA and the Data Protection Act 1998 the ugly sisters).

However, the EIR give effect to the United Kingdom's obligations under the European Directive on Public Access to Environmental Information (Council Directive 2003/4/EC), which in turn derives from one of the three pillars of the Aarhus Convention - namely, access to information in environmental matters. Aarhus itself led on from the Rio Declaration on Environment and Development, the result of the 1992 Earth Summit. This is, to coin a phrase, big international law, and access to environmental information is to be seen as a key factor in facilitating public participation in environmental decision-making. Moreover the EIR are the only one of our domestic access to information laws under which a case has reached the European courts – albeit on a point of relevance to FOIA as well – whether or not public interest arguments raised in favour of different exceptions should be aggregated and weighed cumulatively (Reference for a preliminary ruling from Supreme Court of the United Kingdom (United Kingdom) made on 8 February 2010 - Office of Communications v The Information Commissioner (Case C-71/10)).

"Environmental information" under the EIR must be construed broadly, and includes the following: information on air, atmosphere, water, soil, land, landscape, natural sites, as well as energy, noise, radiation, waste, measures, policies, plans, legislation, agreements and the state of human health and safety as they apply to the environment.

They apply in effect to all public authorities (by contrast to FOIA, which lists those to which it applies) and bodies carrying out functions of public administration. There is an explicit presumption in favour of disclosure of information, and the grounds for refusal are more restrictive than under FOIA.

And while it is still the case that, to a large extent, applicants are unaware of their rights under EIR, and will invoke FOIA (and sometimes take exception when their request is properly dealt with under EIR) this is unlikely to continue indefinitely. Recently it has been noticeable that a number of commercial organisations and pressure groups have begun to take advantage of the regime (in the former group can be counted property search companies, who have established through the IC and appeals to the Information Tribunal that local authorities cannot as a rule charge for providing access to environmental information needed for property searches).

Public authorities (or departments thereof) dealing with planning, highways, waste etc. would be well advised to take a default approach that a request for information they hold is likely to fall under the EIR, rather than FOIA. And all authorities need to be aware firstly of how wide the ambit of the EIR is, and secondly that they must not assume the EIR to be a sub-set of FOIA, but rather a regime in its own right, with its genesis in international environmental law.

Disregard for the EIR could ultimately have major consequences: an apparent failure properly to implement or enforce one of the other "pillars" of the Aarhus Convention has led the European Commission, in the last few weeks, to refer the UK to the European Court of Justice for failing to provide affordable access to justice in environmental cases.

Finally, something often overlooked in the EIR is Regulation 4, which requires public authorities not only to make information available on request, but also to progressively disseminate it electronically and to organise what information it holds in such a way as to promote this systematic dissemination. One wonders how many authorities are doing this, and whether a prominent challenge to a failure to do so will soon emerge.

Jonathan Baines is an Information Rights Specialist at Buckinghamshire County Council. Follow him on Twitter: @bainesy1969

Next Live Webinar - Tim Turner will be doing a live webinar on the Environmental Information Regulations: An Introduction. This is ideal for front line staff as well as new employees. The cost is £20 plus vat which includes slides and a certificate (pdf). Details: **www.actnow.org.uk/content/83**

Environmental Information Regulations

News in Brief

Planning Is (still) an EIR matter
Numerous decisions since Christmas underline the extent to which the Information Commissioner interprets planning and development as being an issue to be dealt with under the EIRs rather than FOI. Whether it's correspondence between the Department for Culture, Media and Sport and the Tate Gallery over the latter's proposed extension **http://bit.ly/kPBcrb** a report about the relocation of Tunbridge Wells' town hall site **http://bit.ly/mdM12l** or even the strengthening and replacement of a bridge in Conwy **http://bit.ly/mFvLMW** each time the Information Commissioner is faced with a question about building, development or planning, he consistently decides for EIR.

It's fair to say that once this has happened, arguments that succeed under FOI may well succeed under EIR. But differences around fees, commercial sensitivity and vexatiousness are significant, and it's vital to remember: planning = EIR.

Fees, FOI and EIR
Continuing the above theme, two recent decisions show that the EIRs offer little comfort for organisations facing expensive requests, despite the apparently tantalising offer of a separate charging regime.

Northumberland Council **http://bit.ly/lq0EG0** were knocked back by the Commissioner in February after levying a charge for staff time in collating and cross-checking requested information. The Commissioner's view is that only photocopying or postage costs can be taken into account when charging for environmental information - you have to swallow other costs however long it takes to identify, locate or retrieve requested information.

Similarly, Nottingham City Council **http://bit.ly/iR7ZFz** appears to have come unstuck with an EIR request for which they actually charged and received a fee of £900. Complex calculations were clearly required to answer a request for the amount of heat sold by an energy company owned by the Council, as it took five days to come up with the required figures. During the investigation, NCC acknowledged that a manifestly unreasonable refusal would have been more appropriate, but nevertheless, the Commissioner found that the staff time required to put the figures together could not be considered 'reasonable'.

So ultimately, what the Commissioner's current position leaves you with is a straight choice – charge only for disbursements (like FOI) or argue that the request is manifestly unreasonable. Our only additional advice is to tease out what you really hold – would a calculation requiring five days' work really be 'held', even in the FOI / EIR sense?

Schools Comply with EIRs!
A less than fragrant EIR request about plumbing reveals that even the smallest of public authorities are required to get to grips with the Environmental Information Regulations. Somerset Bridge Primary School in Bridgewater were asked about the maintenance of its septic tank and sewerage pipes over a defined period: the Decision Notice is here **http://bit.ly/kpE0im**

The information turned out to be relevant to a criminal investigation, meaning that this request was not just the work of a sewerage enthusiast (we've seen everything else in FOI and EIR, so it wouldn't have been a surprise if it was). Though the request was properly handled, it took the intervention of the County Council before the request was resolved.

Act Now will be launching an FOI / EIR pack for both large organisations and schools later in 2011 – keep your eyes peeled!

Prince Charles's Correspondence
Several decisions have surfaced under EIR in recent months on the ever popular theme of 'Who has Prince Charles been writing to, and what has he been writing about?' In the latest cases, government bodies like the Departments for Communities & Local Government **http://bit.ly/lRjgN4** and International Development have been using FOI to refuse to disclose copies of his correspondence, and subsequently being corrected by the Information Commissioner, and told to say no under the EIRs. Act Now's resident EIR anorak would love to know what environmental matters HRH has been writing about, but in a masterstroke that would make Sir Humphrey proud, the Commissioner cannot tell us:

"the Commissioner is not able to explain why he believes the withheld information to constitute environmental information in the body of this Notice without potentially revealing the content of this information."

We're not suggesting that the FOI exemption on Royal Correspondence (Section 37) has been made absolute entirely because of the heir to the throne's missives, but then again, we've never seen any suggestion that the Queen is forever sending out angry letters to public authorities about the lack of facilities for corgis.

FOI/EIR Helpline
Act Now Training provides an FOI/EIR Helpline service. This is designed to supplement your internal FOI/EIR expertise by acting as a "sounding board" or "signpost service" for you to discuss your FOI/EIR requests and possible responses. Through the helpline Ibrahim Hasan will be available to guide you through the relevant area of law, discuss possible exemptions and how to deal with any complaints. At a time of increasing pressure on public sector budgets, the Act Now FOI/EIR Helpline is the most cost effective solution for your FOI/EIR problems. More details at **www.actnow.org.uk/content/25**

Data Protection

Fine By Me
A Commentary of the ICO's Recent Monetary Penalties

Under sections 55A and 55B of the Act the Commissioner may serve a monetary penalty notice on a data controller requiring the data controller to pay up to £500,000.

The Commissioner has to be satisfied that "… there has been a serious contravention of section 4(4) of the Act by the data controller (that's the principles) and it was of a kind likely to cause substantial damage or distress, and it was deliberate and the data controller should have known that there was a risk and failed to take reasonable steps to prevent it"

The first two such penalties were announced on 24th November 2010. On 11 June 2010 a member of staff at the Childcare Litigation Unit of Hertfordshire County Council sent 17 pages of confidential and sensitive personal data by fax to a member of the public instead of to a barrister's Chambers. The documents related to a sexual abuse case involving a child which was being heard at the High Court. The member of staff had input the wrong STD code for Chambers and also failed to use a fax header sheet which would have provided an unintended recipient with details of the sender and instructions on what to do with a misdirected fax.

Subsequently both the data controller and the member of the public reported the security breach to the Commissioner's office. The Commissioner was so concerned about the security breach that two members of staff from the Enforcement team went to the data controller's premises on 24 June 2010 to meet with senior managers.

On the very day the Commissioner was talking to their management team another member of staff in the Childcare Litigation Unit sent 11 pages containing confidential and sensitive personal data by fax to the wrong number instead of the intended recipient of Watford County Court. This time they remembered the fax header and the breach was contained.

The council didn't seem to have any common sense policies in place such as "Ring ahead" or "Confirm receipt" and there seemed to be a reluctance to use these methods. The outcome was £100,000 and the perpetual notoriety of being the first to be fined.
(Trivial Pursuit IPR & Privacy version 2015).

The other fine in November 2010 was to a company called A4e in Sheffield which processes data for amongst others the Legal Services Commission. An employee took home a laptop to work on the data. The only security on the laptop computer was password protection.

On the night of 18th June 2010 the employee was burgled at home with the loss of the laptop holding the sensitive personal data relating to 24,000 clients.

The data included the case type such as debt, welfare, employment, the name, postcode, date of birth and gender of the data subject together with whether or not the data subject was a lone parent, care leaver, carer, a victim of violence, ex-offender, young offender or gypsy traveller.

There was no record of any staff induction training being held although staff had been issued with a selection of policies. Guidance had also been issued to lock laptops away when not in use. The employee left it on a dining table in plain view. Remedial action at this company include mandatory IT security training.

8th February this year saw 2 more fines for 2 more Councils.
Two laptops containing the details of around 1,700 individuals were stolen from an employee's home. Almost 1,000 of the individuals were clients of Ealing Council and almost 700 were clients of Hounslow Council. Both laptops were password protected but unencrypted - despite this being in breach of both councils' policies.. Social Care is the sector.

This was complicated by the fact that Hounslow Council breached principle 6 of the Act by failing to have a written contract in place with Ealing Council. Hounslow also did not monitor Ealing Council's procedures for operating the service securely. Data Controllers who engage data processors to work on their data need a written contract in place and to monitor that contract.

The Commissioner also decided that 3rd principle (adequacy) and 5th principle (retention) had been breached. The data wasn't relevant and had been kept way past its use by date.

Analysing these 4 cases leads to some interesting conclusions. Firstly 3 of the 4 involve laptops which were merely password protected. The laptops were stolen from employee's homes. The data wasn't encrypted despite it being social care and child abuse data which certainly fits into my Schedule 3.

Moral - don't work from home. If your boss makes you work from home then lock your doors and keep your laptop under your pillow when you finish work. Dining room tables are just not quite secure enough. And finally - get encrypted.

The other case falls into the category of 'you couldn't make it up…' An employee tried to use a preset fax number but it was busy so typed in the number themselves and got it wrong. Then when the regulator was dunking his biscuits a week or so later and talking about the cock up another employee did exactly the same thing. They forgot the fax header sheet. They never thought to ring ahead and say a fax is on the way. They just went ahead and did it.

Act Now was at a meeting recently where an ICO speaker talked about monetary penalties and gave us the hard word. He didn't quite wag his finger but he made it clear that they were getting tough. He also said that the onus was on data controllers to self report any significant breaches of the Act and that trying to sweep it under the carpet would result in tougher sanctions. A press release in January 2010 said

"Over 800 data security breaches have been reported to the Information Commissioner's Office in just over two years. The ICO is warning that organisations may face tougher sanctions if they fail to report security breaches which subsequently come to light. Those that try to cover up breaches which we subsequently become aware of are likely to face tougher regulatory sanctions."

Who'd have thought that the woman who put a cat in a wheelie bin or the student who threw the fire extinguisher off Millbank Towers would ever be identified… …but they were.
It is much more difficult to remain anonymous in today's information rich society. If a data controller leaks data into the public domain the public will enjoy reporting the breach to the Commissioner. - See the Hertfordshire case.

The Commissioner's press release of January 2010 says 262 breaches out of 800 were the result of theft, often where the personal information was held on an unencrypted portable device. Prophetic words.

4 fines in 12 weeks around the end of 2010. At this rate and at the current level of fines there will be about 20 a year and £1,000,000 in total. How do organisations avoid this sort of sanction? By using some common sense and putting in place training, policy and compliance with the Act. Once you are on the Commissioner's radar (whether you self report or a member of the public turns you in) you can expect not just a simple breach of principle 7 but a more detailed look at your processing habits. There are after all seven more principles to breach.

Data Protection

Keeping Your PECR Up

You may have noticed a profusion of stories in the tech and mainstream press about changes to arrangements to the use of cookies. Act Now will be offering an online course about the changes, as well as more detailed training and advice on marketing and the law later in 2011, but at the moment, we're holding back for the simple reason that even though we know the changes are coming, nobody can say for certain what the changes are. And the deadline is fast approaching…

The so-called ePrivacy Directive arrived in 2002, and was implemented in the UK in 2003 by way of the snappily titled Privacy and Electronic Communications (EC Directive) Regulations. PECR (say it out loud and giggle) covered a wide variety of issues, some only of interest to telecoms companies. But it also contained wide-ranging provisions for any form of electronic direct marketing, affecting any promotional email, text, fax or phone call. The definition of marketing is wide, such that organisations far from the cut and thrust of commerce are covered by the regulations when they promote their aims and ideals – try to persuade recipients of emails or texts to eat five pieces of fruit and veg a day, and you might as well be selling them a flatscreen TV as far as the law is concerned.

As is usually the case with EU legislation, the 2002 Directive was revisited. As before, the 2009 revision is designed to cover a variety of issues, including many non-privacy matters like making it easier to switch phone provider. However, two elements of the changes are important for those working on privacy and data protection. The first has definitely caught the media's eye, if only because the word 'cookies' afford bored sub-editors the opportunity to run a brace of punning headlines. The requirement states that organisations running websites will need the user's permission before a cookie can be used – a potentially radical change from the status quo, where cookies are planted invisibly on a browser's computer. The fuss is interesting, as

the 2002 Directive always required at least an opt-out, but by insisting on an opt-in, the 2009 Directive increases the pressure.

DCMS has been ambivalent about whether it will hit the implementation deadline of 25th May, while civil servants continue to discuss solutions to the cookie problem with browser manufacturers. Clearly the Government wants to find a simple, flexible, seamless solution to this problem but we don't know what it is yet.

The 15th April press release, **http://bit.ly/edY2iS** also makes clear that the vexed question of the use of cookies for behavioural advertising is still unresolved but firmly on the agenda - Phorm-style tracking software is probably out of the question, but big high-street names are obviously using tracking cookies to show tailored adverts. Your author has been haunted by adverts for a printer he has long since bought, ads clearly fed by a cookie telling websites far and wide about an interest long since dead and gone.

Until the industry discussions are complete, and more importantly, until the Information Commissioner publishes his guidance on how cookies changes will be dealt with, a big question mark hangs over every website operator. Whether it turns out to be a Sword of Damocles or a floating damp squib, only time will tell.

However, the other big change, buried deep in the overall government response to its own consultation **http://bit.ly/he8D9F** on revising ePrivacy (pages 69-70 of the document, fact fans), is a firm commitment to bring PECR into line with DPA's civil monetary penalties. No announcement has been made so far, but the DCMS document is admirably clear on this point – breaches of PECR will be brought into line with the DPA. Presumably, this raises the possibility of the same maximum fine of £500000 being levied for breaches of electronic marketing rules. Without formal confirmation of how this will work in practice, we don't know when the Commissioner will be able to fine, and what for. But those observers who said that the Commissioner lacked the bottle to issue fines under DP have been proved wrong, so the possibility of fines for promotional emails or faxes is coming. We'll watch this space for you.

Fax Awareness Posters

Following the Information Commissioner's fine of £100,000 upon Hertfordshire County Council, now is the perfect time to raise awareness of the dangers of using the fax machine to send sensitive personal data.

To help you do this, Act Now Training has designed an A3 colour poster which can be put up next to every fax machine. This will prompt staff to think carefully about what they are doing and to check they have the right number.

To order your poster(s) (£1.50 each plus vat) please go to our website: **www.actnow.org.uk/contact/**

Don't forget to state how many posters you would like.

Data Protection

PVP Lists and the Slough Case

In December 2010, Slough Borough Council lost a case at the Court of Appeal, having mainly failed in their defence of a defamation case at the High Court in 2009. Slough's use of a widespread warning system was found to have defamed the appellant, especially in the light of Slough's duty to justify any breach of her human rights when putting her details on their violent persons register. The Appeal Court rejected their defence of qualified privilege for the publication, upholding the High Court's decision that sharing or "publishing" the warning as widely as they did was disproportionate. One element of the appellant's case was rejected, in that the High Court did not accept that the council officer investigating the case acted maliciously. Indeed, despite challenging Slough's policy approach, neither judge identified anything but good faith in their staff's actions.

The Incident

The story began with an argument in a Slough park on 11 August 2005. The appellant objected to the behaviour of a child, and an argument with the parents ensued. She complained to Slough's anti-social behaviour co-coordinator, but this went badly, as she did not feel that the staff member dealt with her complaint properly. She admitted later to slamming a phone down so hard to end the conversation that it broke in her hand. Complaints escalated, and one of the claimant's letters to the investigating officer included the sentence, "I am certain I would have physically attacked her if she had been anywhere near me." Subsequently, when meeting with the Council's Head of Public Protection, she said that she hoped the staff member would "drop dead".

The Warning

As a consequence, the Head of Public Protection decided to place the lady on its Violent Persons' Register for 18 months, and gave her a risk rating of medium. As many commentators have noticed, another person on the risk register with the same rating had held a staff member hostage for two hours. No-one was to visit the lady by themselves, and when it transpired that she was hand-delivering letters to Council offices, it was decided that a pair of staff should meet her as soon as she arrived.

Slough's approach was to circulate warnings to Council employees but also to external organisations including the NHS and 50 businesses in the Town Centre Business Initiative and others. An email was also sent to 66 council employees, stating that the claimant had made violent threats. Part of Slough's policy, in line with the DPA, was to inform people that they had been placed on the register. Having received a letter informing her of this fact and making further enquiries about the use and sharing of her information, the claimant decided to sue for damages and the legal process began.

The High Court case:[2009]EWHC 1550 (QB)

Data Protection and Human Rights were discussed in detail before the High Court, and the claimant's human rights were decisive in the outcome, but the action was for defamation. The question for the jury was whether the claimant had been libelled by being placed on a violent person's register, and whether the distribution of the register could be justified.

Essentially, Slough's defence to the charge of defamation was that the labelling of the claimant as violent was justified, and that under qualified privilege, they had a duty to share the information in order to discharge their responsibilities to protect staff safety. Although the investigating officer was not found to have acted with malice, the defence of qualified privilege for circulating the warning widely was not accepted beyond staff in departments with customer-facing staff likely to come into contact with the claimant. The claimant used the right to privacy under Article 8 of the HRA to counter the qualified privilege defence, and the judge accepted that Article 8 required that each element of the register's distribution had to be proportionate.

Many of the departments receiving the warnings were extremely unlikely to meet the claimant (e.g. Child Protection, Youth Offending Team), and some of the external organisations were similar unlikely ever to encounter her. The register was even sent to NHS organisations and local businesses – there was no evidence that the claimant posed any threat to them, even if the Council were correct that her remarks about one officer could be extrapolated as representing a risk to others.

The judgement is also clear that Mr Justice Tugendhat did not believe that the claimant was a violent person: he quietly corrects Slough's approach in his judgement by suggesting that the register should be a "Potentially Violent" Register.

The claimant was awarded £12000 in damages and left, in the judge's words "with her reputation vindicated". It should be noted that the officer who asked for the warning also left the court "without a stain on his reputation".

The Court of Appeal: [2010] EWCA Civ 1171

Slough appealed and lost in December 2010. They advanced the same defence of qualified privilege, but the Court of Appeal again restricted any justification to warnings issued to customer facing staff likely to come into contact with her. Staff working in departments unlikely to meet her and anyone working outside the Council were not entitled to receive warnings. Circulating warnings to other departments and to partner organisations and businesses was not proportionate or fair and so was not covered by the defence of qualified privilege. Publication to anyone not at risk of harm was disproportionate. To publish as widely as the Council breached the claimant's Article 8 human rights, preventing the defence of qualified privilege.

The Court of Appeal rejected the argument that requiring Slough to make a case-by-case assessment for every warning's publication would be disproportionate. The Court of Appeal argued that it could not be disproportionate for Slough (or any public authority) to do what the law requires them to do, both under Human Rights and under the Data Protection Act. Slough lost their appeal. The damages stood, and Slough also face legal bills and a considerable expenditure of human resources.

The Supreme Court: [2010] EWCA Civ 1484

The Supreme Court has refused the Council permission to appeal. This means that the jury's verdict of damages of £12,000 in favour of Ms Clift stands and the correctness of the analysis of the Court of Appeal as to the impact of Article 8 on the law of qualified privilege is confirmed.

Lessons to Learn

1) The nature and extent of a warning has to be judged on an individual basis
2) It is unwise to describe a person as violent – potential violence or risk is a safer label.
3) It is vital to ensure that consistent criteria are applied – Slough's case at the High Court was not assisted by the examples of other more serious cases given the same risk rating at the same time.
4) All data should be accurate
5) Warnings should only be circulated outside your organisation when the specific circumstances demand it.
6) Slough were wrong, proved to be wrong, proved at appeal to be wrong and have been denied the chance to be proved wrong at the Supreme court. What a waste of money.

www.actnow.org.uk/content/81

Data Protection

How Schools Can Comply with Information Law

Do these Acts of Parliament apply to you? It depends on who you are, where you are and how you are funded. A simple answer is that all schools in the UK have to comply with the Data Protection Act. It's a reserved power.

Even this simple answer is complicated by whether you are a state funded school in Scotland in which case the work will be done for you by the local council.

In Scotland state schools have a Parent Council which doesn't have the status of a Board of Governors in England. In Scotland schools do not have to notify - the local council handles it. In England the Board of Governors is responsible for compliance with all law not just information related law.

Private schools whether in the north or the south have to comply with the Data Protection Act. Whether you are a charitable trust or not the law applies to you.

Freedom of Information also has different regimes. In England, Wales & Northern Ireland the education sector comes under the scope of the Act. All schools will have to adopt a publication scheme and handle requests for information themselves.

Except private schools who are outside FOI. But including Academy schools who were brought in at the beginning of this year by the Academies Act 2010. The Act extends to England and Wales but only has application to England. While sections of the Act do technically extend to Wales, you can only establish an Academy in England, so it will have no practical impact in Wales.

Scotland has its own FOI regime and it applies to post 16 education. Any state funded schools who receive requests under the 2002 Act can re-direct the requests to their local council. They will manage the publication scheme and requests for access.

All private schools escape Freedom of Information - unless of course they interact with the state or the public sector in which case requests may be made to public bodies for details of that relationship.

However all schools will be required to consider human rights issues such as the right to privacy and the very new Protection of Freedoms Bill which will become law at some stage which contains items of interest about fingerprinting in schools, CCTV, CRB.

Where to start? Let's kick off with Data Protection.

Notification
It's a legal requirement and there's the possibility of a criminal offence if you don't do it and maintain it. Normally it's just a couple of hour's work a year but you need to be able to prove you've done it if auditors or inspectors arrive. Never heard of it? Hmmm…

Data Processors
Do you allow anyone else to work on your school's data? If so you need to have a contract in place and monitor that contract.

Privacy Notices
The DPA requires schools to provide an oral or written statement, known as a privacy notice, to pupils, parents and staff where they have collected and stored information about them. The primary aim of the notice is to inform an individual about the nature of the personal data that has been collected and stored by the school, and how it has been used. The privacy notice should also provide guidance, setting out how an individual may request access to the information held. Further information on privacy notices for pupils and for members of the school workforce can be found on the ICO website, which sets out the definition of "privacy" notice along with detailed guidance. The Education Department's "model" privacy notice can be obtained from the Department's website.

CCTV and images
Do you hold images whether still or moving of individuals? You need to take account of this in your notification and in your Privacy Notice.

Do you hold images of children on smart cards? Do you allow use of cameras in school? Can you pass images of children or parents to the police? Is there a right of access to video?

Social Media
Can staff & children say things about friends and colleagues in the blogosphere? Can you control this?

Can someone spoof a website that looks like your school website? Can you have defamatory material removed? Who is liable for any defamatory material emanating from your organisation's computers?
There are other hot topics.
• Fingerprinting in school
• Use of email and internet
• Cyber bullying
Maybe it's time you carried out a review of how you comply with the Data Protection Act.

Onto Freedom of Information.
A survey in February 2011 by Action on Rights for Children has highlighted the need for increased awareness of the Freedom of Information Act in schools. The report found that of the 499 schools approached with a freedom of information request only 54% replied. Whilst higher than the previous year (25%) the results show that many schools have a poor grasp of the Act and often simply ignore any requests received.
What are a school's obligations under the Act?
Duty to publish - Duty to confirm - Duty to advise

Information Rights Day
Act Now Training has created what we call an Information Rights Day. For one fee your school will have the services of one of our consultants who will undertake a review of your existing compliance with information legislation, deliver relevant training and make recommendations about how to comply in the future.

A bespoke training package for your LEA
Ask your local Education authority to put on a day for all the schools in your patch. They have the Teacher's Centre or the training rooms. Ask them to invite Act Now Training in and we'll deliver a half day training session covering DP & FOI, take the register, issue certificates to all attendees and handle the feedback sheets with a report back to the LEA. One course can handle 25 delegates. We can deliver as many as you want.

Pyramid Partners training or feeder school friends?
Instead of going it alone why not share the load? If your school is part of a pyramid or a small area with several schools bring the training to you. One fee which is shared around all attendees. Little or no travelling expenses. We provide all you need, you supply the electricity and screen.

Data Protection

Violence Warning Marker Guidance A policy and procedure guide

Providing good quality safety information for your staff has never been more important. In the current climate of cuts and service restrictions, tensions may rise. It is vital that the use and sharing of information about violent incidents or abuse is fair, proportionate and controlled.

Act Now's policy and procedure guide to warnings covers the Data Protection, Human Rights and Confidentiality issues thrown up by the need to balance adequate health and safety for staff with the requirement to handle data responsibly and fairly. The guide provides a clear set of options for how warnings should be shared, what level of information should be available, and what safeguards need to be in place.

With Slough Borough Council losing its case at the Court of Appeal in December 2010 (page 12) for a disproportionate use of warnings data, the Warning Marker guidance is an essential addition to your approach to health and safety.
www.actnow.org.uk/content/81

Cloud Computing

A Practical Guide to the Legal Issues By Renzo Marchini
British Standards Institute - price £30
http://bit.ly/iJPfDM

Cloud Computing seems to be The Next Big Thing. Before venturing into this complex area (both legal and technical) organisations need to understand the benefits and the risks. This book neatly summarises the legal issues which arise when using cloud services, some of which are unique to cloud, others of which are more general but have a unique application to cloud. It covers such areas as security in the cloud, data protection, service levels, and contractual issues. It sets out practical steps to address legal issues both in the regulatory context and in the context of contracts between customers and suppliers. It also deals with issues that arise when the cloud service is used by regulated sectors, such as financial services.

For those new to the cloud the first chapter explains what it is and the different types of cloud solutions. The final chapter looks forward to the future in terms of development of the could and the applicable laws particularly data protection.

This book is an excellent practical resource for those involved in buying or providing cloud services. Lawyers who need to get quickly up to speed on the issues which arise will find it particularly useful. At £30 it is excellent value too.

Cloud Computing and Data Protection: Watch the free webinar by Tim Turner: **www.actnow.org.uk/content/83**

DP News in Brief

Breach at The Co-operative Group leads to exposure of 83,000 records - SC Magazine UK **http://bit.ly/iz54Iu**

BP employee loses laptop containing unencrypted details of 13,000 Deepwater Horizon claimants - SC Magazine UK **http://bit.ly/lMKQHD**

New Data Sharing Code

The ICO has now launched the final version of the data sharing code of practice.

The code, which covers a new statutory requirement, aims to provide good practice advice to organisations that share personal data. It applies to the public, private and third sectors and covers routine or systematic data sharing, as well as one-off requests to share data in specific circumstances.

Biometric Data In Schools

The Protection of Freedoms Bill contains provisions about biometric information in schools. If passed it will require schools to obtain the consent of parents before processing biometric data e.g fingerprints for library books or school meals. Even where parents approve the child may still object.

Action on Rights for Children (ARCH) have a very interesting briefing on the subject: **http://bit.ly/hCRhRi** It welcomes the proposal to introduce consent into the process of taking children's biometric data, but suggest that ensuring any consent is valid and informed will present a considerable challenge.
Please get in touch if you want a briefing note on this subject.

ICO Personal Information Promise

The ICO is urging organisations and government departments to sign up to the Personal Information Promise. Signing the promise allows organisations to show the wider public that they are taking their obligations under the Data Protection Act seriously. More than 1,200 organisations have already signed up to the promise since its launch in January 2009 - ranging from small local authorities to household names from the private sector.

CCTV Consultation

The Home Office is currently consulting on a new code of practice on the use and regulation of CCTV and other surveillance camera systems including Automatic Number Plate Recognition. The consultation covers data protection issues, such as the retention of data, and the future roles of the Information Commissioner and the new Surveillance Camera Commissioner.

Once published, the code's provisions will become a statutory duty for police forces and local authorities in England and Wales, with the aim that its standards will be adopted more widely.

If you are interested in sharing your views, please visit the Home Office website - **http://bit.ly/fgYMCY** The closing date for responses is 25 May 2011

Courses in Bristol

Act Now is running more Data Protection, Freedom of Information and Information Sharing Courses in Bristol with Philip Bradshaw in the Winter/Spring 2011 Season. For more information please see:**http://bit.ly/jJJz7k**

Data Protection

Data Protection Policy and Guidance Pack

Data Protection and Information Security Resources for your organisation

The Information Commissioner is now using his powers to fine; media interest in data protection stories has never been higher, and the public's expectations remain as strong as ever. With email, blogs, Twitter and Facebook at their fingertips, sensitive information can go airborne before you even know it. Meanwhile, with pressure on spending, posts going empty and perhaps even DP people going as well, the ability to keep on top of a Data Protection landscape that never stops changing may be difficult to achieve. The Act Now Policy and Guidance Pack will help your organisation deal with all this.

The Policy and Guidance Pack is designed to cover a range of Data Protection issues and challenges in one document. From decisive policies that will define your corporate approach to a range of simple procedures, agreements and guidance, the aim is to provide a stack of documentation ready for adoption, but flexible enough to be adapted for your needs. You can put them in place now, you can completely rewrite them, or we can adapt them for you. Plug the gaps or clear the decks and use them all, it's up to you.

As the current UK cost of two faxes sent to the wrong place is currently £100,000, the Act Now Policy Pack could be your best investment.

More details:

www.actnow.org.uk/content/82

COMING SOON:

A POLICY PACK FOR SCHOOLS

Data Protection Helpline

Public authorities are increasingly receiving complex and time consuming Data Protection requests. These involve consideration of a number of Data Protection exemptions as well as relevant Information Commissioner and Tribunal decisions. Internal legal departments are often over stretched and dedicated Data Protection practitioners are hard to recruit. External legal advice in this area is very expensive and there are very few experts in this field with real experience of advising the public sector.

The Act Now DP Helpline is designed to supplement your internal expertise by acting as a friendly advisor for you to discuss your Data Protection and Privacy issues and avoid attracting the attention of the Information Commissioner. Our experts will guide you through the relevant sections of the Act and make recommendations about your response to difficult DP situations.

Please click here for more info and subscription details

www.actnow.org.uk/content/25

Junk Communications How to Fight Back and Get Results

Section 12 of the Data Protection Act states that "an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease or not to begin processing for the purposes of direct marketing personal data of which he is the data subject."

Turned into plain English you can object to any marketing (the Act says "communication by any means") targetting you at your address or personal phone number. It is an absolute right.

The marketer must respect your preference. If they don't you can apply to a court for an order to force the marketer to comply. There are however some halfway houses known as preference services which allow you to express your objection to Junk.

Marketing itself is very broad - the promotion of an idea or philosophy, trying to influence your behaviour, asking for donation. There are many marketing channels and many styles.

But you can fight back. Your staff have a feeling that junk is handled under Data Protection so don't let them down. Mug up on it. Have the answers to their queries at your fingertips.

READ THE FULL ARTICLE:

www.actnow.org.uk/content/46

RIPA/RIPSA Helpline

Local authorities and other public sector organisations are increasingly doing complex and time consuming covert investigations to tackle benefit fraud, licensing problems, trading standards offences, anti social behaviour and environmental health problems.

The Act Now RIPA/RIPSA Helpline is designed to supplement your internal surveillance law expertise by acting as a "sounding board" or "signpost service" for you to discuss your covert surveillance operations. Our experts will guide you through the relevant area of law; discuss possible legal tactics and how to complete the relevant standard Home Office forms. The helpline is managed by Ibrahim Hasan who is renowned throughout the UK as a leading surveillance law expert.

Watching You Watching Them

The Protection of Freedoms Bill and Local Authority Surveillance

By Ibrahim Hasan

The long awaited Protection of Freedoms Bill is currently going through Parliament. If passed in its current form, it will curtail local authorities' powers to carry out surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) and to deploy CCTV cameras. The Bill implements Home Office recommendations contained in a review of counter-terrorism and security powers, published on 26th January 2011.

Magistrates' Role

Chapter 2 of Part 2 of the Bill (clause 37 and 38) amends RIPA so as to require local authorities to obtain the approval of a magistrate for the use of any one of the three covert investigatory techniques available to them under RIPA namely Directed Surveillance, the deployment of a Covert Human Intelligence Source (CHIS) and accessing communications data. An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the magistrate is to ensure that the correct procedures have been followed and the appropriate factors have been taken account of. The new provisions allow the magistrate, on refusing an approval of an authorisation, to quash that authorisation.

Communications Data

Chapter 2 of Part 1 of RIPA allows local authorities, as well as others, to access communications data about an individual from any Communications Service Provider (CSP) (e.g. a telephone or mobile phone service provider).

A new section 23A will be added to Chapter 2. An authorisation or notice to obtain communications data from a CSP shall not take effect until a magistrate has made an order approving it. The magistrate must be satisfied that:

a) There were reasonable grounds for the Designated Person (the person authorising the obtaining of the data) within the local authority to believe that obtaining communications data was necessary and proportionate and that there remain reasonable grounds for believing so.

b) The Designated Person was of the correct seniority within the local authority in accordance the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) i.e. Director, Head of Service, Service Manager or equivalent.

c) The granting or renewal of the application was only for the prescribed type of communications data to be acquired for the prescribed purpose as set out in the above Order (i.e. subscriber and service use data (e.g. mobile phone subscriber information and itemized call records) to be acquired only for the purpose of preventing or detecting crime or preventing disorder)

d) Any other conditions set out in an order made by the Secretary of State under Chapter 2 of Part 1 of RIPA are satisfied (none at present).

Directed Surveillance and CHIS

Clause 38 of the Bill makes similar provision for magistrate approval of local authority authorisations for the use of Directed Surveillance and the deployment of a CHIS. It does this by adding a new section 32A to Part 2 of RIPA.

Directed Surveillance is often conducted by local authorities to, amongst other things, investigate a benefit fraud or to collect evidence of anti-social behaviour. Typical methods include covertly following people, covertly taking photographs of them and using hidden cameras to record their movements. A typical example of a CHIS, in a local authority context, is an informant using his relationship with his employer to regularly disclose information about benefit fraudsters working in a factory.

Once again the internal authorisation for such surveillance methods is not to take effect until such time (if any) as a magistrate has made an order approving it (section 32A(2)). Approval can only be given if the magistrate is satisfied that:

a) There were reasonable grounds for the authorising officer approving the application to believe that the Directed Surveillance or deployment of a CHIS was necessary and proportionate and that there remain reasonable grounds for believing so.

b) The authorising officer was of the correct seniority within the organisation i.e. a Director, Head of Service, Service Manager or equivalent as per the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) ("the 2010 Order").

c) The granting of the authorisation was for the prescribed purpose, as set out in the 2010 Order i.e. preventing or detecting crime or preventing disorder.

d)Any other conditions set out in any order under Part 2 of RIPA are satisfied (none at present).

In addition to the above, where the authorisation is for the deployment of a CHIS, the magistrate must be satisfied that :

e) The provisions of section 29(5) have been complied with. This requires the local authority to ensure that there are officers in place to carry out roles relating to the handling and management of the

CHIS as well as the keeping of records (as per the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725)).

f) Where the CHIS is under 16 or 18 years of age, the requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) have been satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation. Note that the authorisation of such persons to act as a CHIS must come from the Chief Executive.

g) Where the application is for the renewal of a CHIS authorisation, a review has been carried out by the local authority and the magistrate has considered the results of the review.

The new provisions make it clear that the authorising officer is not required to apply in person and there is no need to give notice to either the subject of the authorisation or their legal representatives (Section 23B (2) and 32B(2)). This reflects the covert nature of the exercise of the investigatory powers under RIPA.

Directed Surveillance and the Serious Offence Test

The Home Office Review also recommended that where local authorities wish to use RIPA to authorise Directed Surveillance, this should be confined to cases where the offence under investigation carries a custodial sentence of six months or more. This recommendation is to be put into effect by an order to made under section 30(3)(b) of RIPA.

The new RIPA codes of practice, which will accompany the changes to the local authority surveillance regime, will spell out precisely how the magistrate approval process will work. The changes will have a profound impact on local authority investigators especially in Benefit Fraud and Audit. The added scrutiny of authorisation forms by magistrates will increase the importance of staff training and guidance on completing such forms correctly (see page 17).

Surveillance Law and Privacy

The New CCTV Regime

Chapter 1 of Part 2 of the Protection of Freedoms Bill makes provision for the further regulation of surveillance camera systems. These are defined as Closed Circuit Television (CCTV), Automatic Number Plate Recognition (ANPR) and other surveillance camera technology operated by the police and local authorities.

Clause 29 of the Bill requires the Secretary of State to prepare a code of practice in relation to such systems. This must include guidance in relation to the development or use of such systems, and the use and processing of information derived from them. It may also include provisions about:

- considerations as to whether to use surveillance camera systems
- types of systems or apparatus
- technical standards for systems or apparatus
- locations for systems or apparatus
- the publication of information about systems or apparatus
- standards applicable to persons using or maintaining systems or apparatus
- standards applicable to persons using or processing information obtained by virtue of systems
- access to, or disclosure of, information so obtained
- procedures for complaints or consultation

Clause 33 of the Bill provides that the police and local authorities must have regard to the Code if they operate or intend to operate any surveillance camera systems covered by the Code. The Secretary of State may by order designate other bodies as being required to have regard to the Code. Failure to adhere to the Code will not in itself render an organisation liable to legal proceedings, but the Code is admissible in civil or criminal proceedings. The Code could also be enforced by way of judicial review in the High Court by any agrieved person.

On 1st March 2011, the Home Office launched a consultation on the contents of the Code. The deadline for responses is 25th May 2011. The consultation paper can be downloaded from the Home Office website:
http://bit.ly/fgYMCY

Of equal note is the creation of a new Surveillance Camera Commissioner (clause 34) who will encourage compliance with the Code, review its operation, and make annual reports about the Code and its operation to Parliament.

The CCTV provisions in the Protection of Freedoms Bill add a completely new layer of control over the use of CCTV by local authorities and the police. One has to question whether they are necessary, especially at a time of huge public sector budget cuts. CCTV is already subject to controls under both the Data Protection Act (DPA) and (if covert) Part 2 of RIPA. There is already a CCTV Code under the DPA which is enforced by the Information Commissioner. Will the new code and Commissioner take precedence? Furthermore in the age of You Tube, Flickr and Facebook, some believe that the Government should have at last focused equal attention to regulating private individuals' and the private sector's use of CCTV and video technology.

RIPA Update Workshops

Bristol, Belfast, London and Manchester £265 + vat

Our speakers will be discussing all the latest changes in detail giving you a head start in implementing them. Full details on our website.**www.actnow.org.uk/courses/RIPA/Surveillance_Law**

RIPA Forms Guidance Manual (version 3)

Act Now Training is pleased to announce that version 3 of the RIPA Forms Guidance Manual has now been published. It has been fully revised in the light of the new RIPA Order and Codes of Practice, which came into force on 6th April 2010. The Home Office forms still make reference to the old codes. Our forms are reproduced with references to the new codes.

Version 3 (April 2010) of the Guidance includes each RIPA form with:

- Detailed notes on how to complete each section
- References to the new RIPA Codes and Order
- References to the OSC Procedures & Guidance

Other useful documents including:

- A detailed briefing note on the new RIPA codes & the changes they make to the local authority RIPA regime
- Revised colour flowcharts to help officers decide what type of surveillance they are undertaking
- A list of common mistakes to avoid
- A suggested template form to be used when doing non RIPA surveillance, not available elsewhere

For more details: http://www.actnow.org.uk/content/26

You can also download an evaluation version.
A Scottish version (RIPSA) is also avaiable.
There is a 33% discount for those of you who bought earlier versions.

Act Now at your Service

Act Now Job Bank

The public sector budgets cuts have forced many organizations to reorganise and restructure their workforce. Act Now intends to maintain a list of information governance vacancies and job seekers with a view to doing some match making. This will be done with the consent of the parties and for no charge. If you are an information governance professional looking for a job or a public authority with a suitable vacancy, please get in touch with us. We will also advertise the vacancies in our newsletter and on our website for free.

Latest Vacancies
Orbit Group Ltd
http://bit.ly/mbXSQQ
Email: Paula.Tighe@orbit.org.uk

Austerity Measures

Times are hard. Budgets are being cut, staff and expertise are being lost. And at the same time, pressure from the Information Commissioner is only increasing.

Four monetary penalties for Data Protection breaches have been issued in the last six months, one totalling £100,000, while enforcement action, formal monitoring and naming and shaming have become part of the ICO's standard approach for Freedom of Information. Indeed, the Information Commissioner's powers are actually increasing, with new powers to impose monetary penalties and issue information notices for third parties under the Privacy and Electronic Communications Regulations, raising the possibility of fines for marketing and cookies.
In short, information rights are hardly losing their sting. Act Now has a number of different offerings to suit your budget. See the back of this newsletter for further details.

IN HOUSE TRAINING

Act Now trainers can also deliver in-house customised training at your site. At a time of increasing pressure on public sector budgets this may be the most cost effective solution to your training needs.

In the last three months we have done in house training on FOI, EIR, DPA, Data Sharing and RIPA for, amongst others, the Association of Greater Manchester Authorities, North Yorkshire Fire and Rescue, Harrogate Council, Liverpool City Council, SILG Commercial Lawyers SIG, Kent County Council and many others.

If you would like a quote to bring the trainer to you please use our online enquiry form:
http://www.actnow.org.uk/enquiry/

Connect with Act Now

If you would like all the latest developments in Information Law delivered direct to your e mail or smartphone then follow us on Twitter:

http://twitter.com/ActNowTraining

We are also on LinkedIn.

and Facebook:

ACT NOW TRAINING LTD, 64 BRADFORD ROAD, DEWSBURY WF13 2DU
TEL 01924 451054, FAX 01924 451129

ISEB Certificate in Data Protection
with Paul Simpkins & Tim Turner

Edinburgh	Starting 6th September 2011
Manchester	Starting 23rd November 2011

Full details available on www.actnow.org.uk/content/30

ISEB Certificate in Freedom of Information
with Ibrahim Hasan & Tim Turner

Manchester	Starting 1st September 2011

Full details available on www.actnow.org.uk/content/31

Data Protection Act 1998: An A-Z Guide
with Paul Simpkins & Phil Bradshaw

London	12th July and 8th November
Manchester	14th June and 15th November
Bristol	22nd November
Edinburgh	22nd November
Belfast	21st June

A complete guide to the Data Protection Act 1998 and its codes of practice. Suitable for beginners.

FOI/FOISA: An A-Z Guide
with Ibrahim Hasan, Tim Turner, Allan Graham & Phillip Bradshaw

London	13th July and 9th November
Manchester	15th June and 16th November
Bristol	23rd November
Edinburgh	23rd November
Belfast	27th May

A complete guide to the Freedom of Information Act 2000 and its codes of practice. Suitable for beginners

Data Protection Update
with Tim Turner

London	13th December
Manchester	7th December
Edinburgh	30th November

Analysis of the latest DPA cases, developments and news from the ICO. Suitable for previous DP delegates.

Handling Requests for Personal Data
with Tim Turner

London	5th October
Manchester	24th May and 12th October
Edinburgh	2nd November

How to handle requests for personal data under section 7 of DPA and section 40 of FOI (S.38 FOISA).

FOI/FOISA Update
Latest Decisions & the Public Interest Test
with Ibrahim Hasan, Tim Turner, Allan Graham & Phillip Bradshaw

London	20th September
Manchester	27th September
Bristol	9th June and 14th December
Edinburgh	28th June

An update on the latest Commissioner, Tribunal and court decisions under FOI and FOISA (Edinburgh).

RIPA and RIPSA
Covert Surveillance Update
with Ibrahim Hasan & Steve Morris

London	24th November
Manchester	17th November
Belfast	19th May and 1st December
Bristol	26th May and 17th November
Edinburgh	10th November

An update on the latest developments in the law and practice of covert surveillance under RIPA and RIPSA.

FOI, Contracts & Commercial Confidentiality
with Ibrahim Hasan

London	1st November
Manchester	7th December

How to handle requests for commercially sensitive information under FOI section 43 and 41.

Email & Internet Monitoring
with Ibrahim Hasan

Manchester	6th July
Edinburgh	4th July

A thorough examination of the law and practice in this area including what to include in HR policies.

Multi Agency Information Sharing
with Ibrahim Hasan & Phillip Bradshaw

London	23rd June and 29th November
Manchester	29th June and 3rd November
Bristol	27th October

An interactive workshop examining the laws which apply to this complex and controversial area.

The FOI/FOISA
Records Management Code of Practice
with Philip Jones

London	30th November
Manchester	8th June and 15th November
Edinburgh	21st November

A thorough examination of the FOI S.46/FOISA S.61 Records Management Code of Practice.

Home Office RIPA SPoC Accreditation
Two day course (£545 + vat)
with Ibrahim Hasan

London	24th & 25th May
Manchester	25th & 26th October

A Home Office accredited two day course essential for those wanting to act as a SPoC for their organisation.

RIPA: Accessing Communications Data
Designated Person / Investigator Workshop
with Ibrahim Hasan

London	13th December
Manchester	1st December

A refresher/update for SPoCs and Designated Persons on the latest news and guidance in this area.

Environmental Information Regulations
with Tim Turner

London	15th December
Manchester	8th December

A thorough examination of EIR, the latest cases and the CON29 search information issue.

Information Security Update
with Andrea Simmons

London	10th November
Manchester	2nd November

A workshop to help implement the IS Framework, including the Seven Principles of the HMG SPF.

Act Now Training is the UK's leading provider of seminars and workshops on all aspects of **Data Protection**, **Freedom of Information**, **Surveillance Law** and **Records Management**.

SPEAKERS	Led by **Ibrahim Hasan** and **Paul Simpkins** (our directors), our speakers are well known experts with many years of public sector experience.
ISEB	Act Now is one of the UK's leading providers of ISEB courses leading to the Certificate in Data Protection and Freedom of Information. We have an overall pass rate of over 80%.
INHOUSE TRAINING	We are the leading providers of in house training on all aspects of information and surveillance law. Our clients include most local authorities in the UK as well as many government departments, NHS bodies and public sector agencies.
ACCREDITATION	All our workshops are accredited by the Solicitors Regulation Authority (SRA) and the Institute of Legal Executives (ILEX) for CPD Credits. Delegates receive a certificate of attendance.
VENUES	Act Now's external workshops are held throughout the UK at top quality city centre hotels in London, Manchester, Bristol, Edinburgh and Belfast. Refreshments and lunch are provided on the day and courses run for a full day from 10am to 4pm.
HELPLINES	We now offer a range of dedicated help lines to assist busy public sector information professionals and in house lawyers deal with information and surveillance law matters.
FOI PODCAST	This is the only FOI podcast of its kind in the UK and has been mentioned in The Times newspaper and numerous other blogs. In each episode Ibrahim discusses the latest decisions from the Information Commissioner and the Tribunal.
ONLINE TRAINING	We provide CPD accredited, live and fully interactive webinars on information rights legislation (e.g. DP, FOI, EIR and surveillance law (RIPA and RIPSA)). The webinars are ideal for training frontline staff.
POLICIES AND GUIDANCE	We have a range of policy documents and guidance including a DP policy pack, Potentially Violent Person (PVP) procedure and RIPA forms guidance.

FIVE EASY WAYS TO BOOK

TELEPHONE	**01924 451054**	**EMAIL**	**info@actnow.org.uk**
FAX	**01924 451129**	**POST**	**Act Now Training Ltd 64 Bradford Road West Yorkshire WF13 2DU**
ONLINE	**www.actnow.org.uk**		

iseb Accredited Training Organisation

FOLLOW US ON twitter

LinkedIn