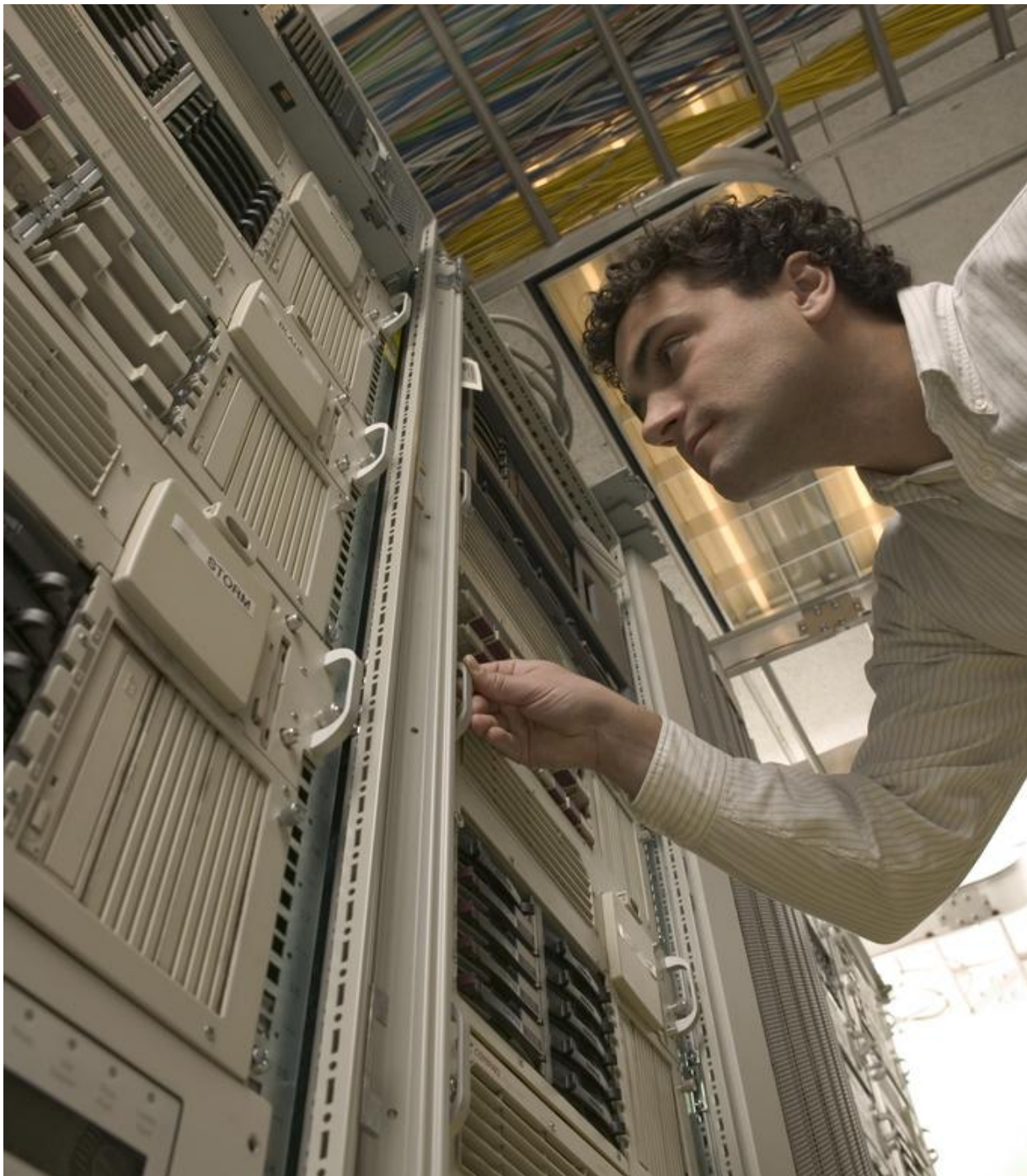


August  
2011

## Report on Cloud Computing and the Law for UK FE and HE (An Overview)

**Please Note:** This guidance is for information only and is not intended to replace legal advice when faced with a risk decision.



# Report on Cloud Computing and the Law for UK FE and HE

This report is intended to survey the legal issues which are likely to arise where a UK college or university is deciding to adopt a cloud computing delivered ICT service, and the legal issues which may arise in the operation of such a service

This publication is part of JISC Legal's Cloud Computing and the Law toolkit. Access the entire toolkit at: [www.jisclegal.ac.uk/Themes/CloudComputing.aspx](http://www.jisclegal.ac.uk/Themes/CloudComputing.aspx). For further information on JISC's work on cloud computing, visit

<http://www.jisc.ac.uk/whatwedo/topics/networkinfrastructure/cloudcomputing.aspx>

---

## Key Points

- Consideration of legal risk must be considered in deciding whether a cloud computing solution is appropriate for any particular institution's needs
- There are no legal issues which constitute an outright bar to the adoption of a cloud computing solution
- Issues which are likely to be of key concern, and which may require mitigating action, are dealing with under-developed standard terms and conditions, the data protection requirements, and data security issues.

---

## Contents

<b>1. Introduction</b> .....	<b>3</b>
<b>1.1. Benefits and Challenges</b> .....	<b>4</b>
<b>2. Cloud Computing and the Law</b> .....	<b>5</b>
<b>2.1. Data Security and Compliance</b> .....	<b>5</b>
<b>2.2. Jurisdiction</b> .....	<b>9</b>
<b>2.3. Confidentiality</b> .....	<b>10</b>
<b>2.4. Freedom of Information</b> .....	<b>11</b>
<b>2.5. Intellectual Property Rights</b> .....	<b>11</b>
<b>2.6. Equality and Accessibility</b> .....	<b>14</b>
<b>2.7. Contracts</b> .....	<b>14</b>
<b>3. Summary</b> .....	<b>15</b>

## 1. Introduction

For the purposes of this report, cloud computing will be taken to mean software, platforms or infrastructure provided as a service by a pool or network of servers. In most cases, such services will be provided by an external, third-party via the internet, and as a commercial service. It is recognised, however, that 'internal' cloud computing provision is also possible as a configuration of the organisation's own server resources, or can be provided by a collective organisation of which the institution is part.

Cloud computing is fast becoming the most pervasive delivery method for IT services across the public and private sectors in the UK. Benefits such as a wide range of customised solutions and increased efficiency savings make cloud computing an attractive prospect. Alongside these benefits are some legal implications to consider. These are not necessarily 'new' legal issues for institutions, and there is no specific 'cloud computing' law; rather, as with any change in a core service delivery model, this may mean existing legal duties, regulations and considerations have to be reframed to fit the new model. As the cloud computing market stabilises, the risks will become clearer and standards set. The law may eventually be updated where required to meet the new technological needs. The term 'cloud computing' refers to internet based computing that allows organisations to access a pool or network of computing resources that are owned and maintained by a third party via the internet.

The key characteristics of cloud computing are:

- Independence of location due to the use of remote servers
- Services that are accessed by users on demand through a broadband network.

These services can include applications, computing power and operating systems, or the general outsourcing of ICT processes and services. Cloud computing solutions can be bespoke or bought off the shelf. There are a number of different types of "cloud", depending on how the cloud is deployed or the type of network it covers, and these include public clouds, private clouds, community clouds and hybrid clouds. Each type of cloud and cloud service provision (e.g. PAAS, IAAS, and SAAS) has

different benefits and challenges and suits different business models and purposes. All have broadly similar legal issues to consider - it is the level of control, risk and ability to comply with the law which may vary.

Familiar examples of cloud providers are Google Apps, Amazon Web Services (which includes the Amazon S3 simple storage service) and Microsoft Windows Azure.

### 1.1. Benefits and Challenges

Overall benefits of cloud computing include:

- high flexibility
- potential for greater efficiency of service
- reduction in cost
- increased scalability (as you are less affected by peaks in usage)
- can be set-up quickly
- can be procured with relatively little commitment

Cloud computing can also facilitate a collaborative, location and time independent working environment with less onsite space needed for servers.

The main challenge from a legal perspective is some loss of control, as would be expected with the outsourcing of any core organisational function. This can impact on information governance and compliance with UK legislation. There is currently some lack of standardisation in the cloud computing industry due to its infancy and this could have some issues for interoperability, or create a risk of inadvertently becoming tied or locked in to one cloud provider. There may not always be a financial advantage and there could be hidden costs in implementing the cloud solution which best suits your purpose and risk approach with existing infrastructure. This may require a level of expertise within the organisation to operate and audit.

## 2. Cloud Computing and the Law

The legal implications of using cloud computing solutions are broadly similar to those for any outsourcing arrangement with a third party. One major difference in using a cloud provider arises from the flexibility and movement of data between servers that may be located in various parts of the world. This makes it difficult to identify which law applies at any given time to the data, particularly as the data may also have been fragmented to suit particular cloud availability or capability. However, the key point is to consider the legal implications of using the cloud at the outset when planning your cloud provision to ensure that you have considered the risks and their management and mitigation to a satisfactory level for your institution.

Key legal areas to consider with cloud computing are:

- Data security and data protection compliance
- Jurisdiction
- Confidentiality
- Freedom of information
- Copyright
- Equality legislation
- Law of contract (including contract enforcement)

### 2.1. Data Security and Compliance

There is ongoing legal research and argument that data protection law is outdated and is currently not a good fit with cloud computing. In particular, it is argued that unreasonable demands are being placed on data controllers wishing to transfer data overseas. Furthermore, due to the nature of the cloud and the amount of control the cloud provider may exert over the data and its movement, there is a view that a cloud provider is also the data controller (and that therefore an institution is effectively passing its data to a third party). However, despite the legal debate, the current position in UK law is that an institution will usually be considered the data controller with regard to its personal data being processed using cloud computing facilities. As such, your institution will need to comply with the Data Protection Act 1998.

The Data Protection Act 1998 (DPA) applies to the 'processing' of personal data. The definition of processing is broad and will include transfer, storage, alteration, and deletion i.e. it covers all interaction with the data. The DPA applies to personal data only. This is defined as data relating to a living individual from which you can identify the individual or which, if combined with other data, may identify the individual.

In using a cloud service, an institution will usually be the data controller responsible for compliance with the DPA when processing personal data and the cloud provider will be the data processor. The cloud provider as data processor should act in accordance with the agreed terms under the contract with your institution in order to ensure compliance with the DPA.

Institutions will also have other confidential data which is not personal data, for example, sensitive financial planning data which it will consider as confidential or highly sensitive and requiring adequate protection from unauthorised access or release. This will be discussed in more detail under confidentiality below.

Whether outsourcing data processing to a processor (i.e. the cloud provider) or processing the information within the institution, a data controller has eight data protection principles to adhere to in order to comply with the DPA. The principles are intended to provide a technology-neutral framework for balancing an organisation's need to make the best use of personal data, while safeguarding that information and respecting individuals' private lives.

The eight data protection principles state that personal data must be:

1. Fairly and lawfully processed.
2. Processed for limited, stated purposes.
3. Adequate, relevant and not excessive.
4. Accurate and up-to-date.
5. Kept no longer than necessary.
6. Processed in accordance with the individual's rights.
7. Secure.
8. Not transferred to a country outside the European Economic Area unless that country has adequate data protection itself.

There are also additional conditions to meet to ensure compliance and these depend on whether the data is personal data or sensitive personal data. As stated above, 'Personal data' is any information, including photographs or other images, about an identifiable living individual regardless of the format of information. The overriding test is whether the information in question on its own or when combined with other information, is significant biographical information that would identify the individual. 'Sensitive personal data' includes information regarding an individual's race or ethnic origin, and physical or mental health. JISC Legal has detailed information on data protection at: [www.jisclegal.ac.uk/LegalAreas/DataProtection.aspx](http://www.jisclegal.ac.uk/LegalAreas/DataProtection.aspx)

Whilst compliance with all the data protection principles is required, it is the seventh and eighth data protection principles highlighted above which are most problematic for UK institutions in using a cloud provider.

### **Security of Personal Data**

An institution as data controller has an obligation to ensure that the cloud provider has adequate measures in place to protect personal data securely against unauthorised or unlawful processing, and against accidental loss, destruction, and damage. There is no set definition of what would constitute 'adequate security' and the Information Commissioner's Office (ICO), which is responsible for enforcing compliance with the DPA, suggests a risk based approach. The ICO has an overview of security requirements at:

[www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/principle\\_7.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx)

There is also a Data Protection Good Practice Note: Security of Personal Information available at:

[www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/security%20v%201.0\\_plain\\_english\\_website\\_version1.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf)

When choosing a cloud provider, your institution should enquire as to how that provider handles personal data. It should also investigate assurances offered, responses to breaches, reactions to UK DPA requirements, and use of security measures such as encryption. It is important to ascertain which other third parties

have access to the data, for example, those to whom elements of the cloud service provided is subcontracted e.g. an IAAS or PAAS.

Your institution will need to consider whether the security level offered meets both the institution's requirements and that of the DPA. It will also need to ensure that the terms of the contract with the cloud provider reflect these requirements.

### **Transfer of Data to a Country Outside the EEA**

The DPA states that personal data is not to be transferred outside the EEA (European Economic Area) unless there is an adequate level of protection for the data subjects regarding the processing of personal data.

Cloud providers intrinsically store and move data around multiple servers potentially situated in a number of jurisdictions which may very likely be outside the EEA. This activity will breach the DPA unless these jurisdictions have adequate security measures in place.

Compliance may be achieved through using EU approved contract terms with your cloud provider, or a cloud provider in the US who has signed up to the Safe Harbor provisions, or by getting informed consent from the data subjects to transfer it to an 'unsafe' location (which is not a recommended solution).

The ICO has more information on transfer of data at:

[www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/principle\\_8.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx)

The Cloud Security Alliance (CSA) has various research initiatives on security in the cloud including an initiative to create standards to measure cloud computing security.

Please visit: [cloudsecurityalliance.org/](http://cloudsecurityalliance.org/)

#### **Key point**

Data protection compliance remains an institutional obligation in the cloud. Check your cloud provider's position on security, data transfer, and compliance with EU data protection law.

## 2.2. Jurisdiction

Broadly speaking, a UK court can only rule on a dispute if it has jurisdiction and similarly, law enforcement agencies such as the police may only operate where they have agreement or jurisdiction. To complicate matters, there are a number of international agreements relating to jurisdiction. Varying rules as to which jurisdiction applies have been agreed upon depending on the area of law and nature of the dispute. In addition, there may be layering of provision, for example, a cloud provider may outsource some of his service provision e.g. data storage or infrastructure. This will make it more difficult to ascertain where the information is at any given time. Also, local laws may apply which permit wider access than you anticipated.

A well publicised example of this is the US Patriot Act. The Patriot Act is intended to assist terrorism prevention in the US and permits access to data by the US Federal Government in certain circumstances, mainly in the interest of national security.

The assumption is that in using a cloud provider, data will be moved. However, without knowing the jurisdiction to which it is moved, it will be difficult to assess the jurisdiction and its suitability. If this issue is not discussed and agreed at the outset, the result may be protracted disputes. There are examples of such disputes involving Google and Yahoo.

Law enforcement agencies may also experience difficulty in (a) tracking down information and (b) finding information in jurisdictions where they have no authority.

There is further information available in the paper Law Enforcement Access in a Cloud Environment available from the QMUL Cloud Legal Project at:

[www.cloudlegal.ccls.qmul.ac.uk/index.html](http://www.cloudlegal.ccls.qmul.ac.uk/index.html)

### **Key point**

Despite best efforts, a dispute may arise with your cloud provider. Use a well established cloud provider and if possible find out where their servers are located, assess suitability and agree which law applies.

## 2.3. Confidentiality

The flow and movement integral to cloud computing may make it difficult to locate the data at any given time and difficult to ascertain whether it is in a secure location. It may often be difficult to assess which third parties have access or access capability to the data as this may change with new or additional providers, services and server locations. Information handled in a cloud environment, although not personal data, may be confidential in nature. An example would be an institution's dealings with a commercial research collaborator (e.g. a pharmaceutical company), where your institution may be subject to contract confidentiality clauses which constitute a legal obligation of confidence. If confidentiality of information is crucial, then risk decisions will need to be made as to its security. Although it might be implied that the cloud provider will maintain confidentiality, it may be desirable to state clearly in the contract terms what obligations of confidentiality are owed between the parties.

### Key Point

Identify confidential material and assess whether the cloud is the most suitable place to store and work with it. Check that the cloud provider's security and access terms meet your needs.



## 2.4. Freedom of Information

Institutions in the UK, as public authorities, have a legal duty to comply with freedom of information (Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002) and other related legislation such as the environmental regulations. If a request is made to an institution for information and your institution holds the information, it is required to release it to the requester within 20 days, unless an exemption or an exception applies. It is likely that even although the information may be stored in the cloud, an institution will still be deemed to be holding it for the purpose of FOI. It is therefore necessary to ensure that access to information is timely - outage, failure, and back-up details should be assessed when choosing your cloud provider.

### Key Point

Institutions will need to be able to access information stored in the cloud in order to comply with Freedom of Information legislation.

## 2.5. Intellectual Property Rights

Intellectual property rights (IPR) are, broadly, rights granted to creators and owners of works that are the result of human intellectual creativity. These works can be in the industrial, scientific, literary or artistic domains. The types of IPR considered here are copyright, the database right, and patents.

Essentially, copyright protects original works, including films or broadcasts, and the typographical layout of published editions. This will include works such as teaching and research materials and blogs. Software (computer programs) and databases may be protected as literary works, in addition to other possible rights such as database right.

A college or university will usually be the owner of copyright works created by its staff, unless there is an agreement otherwise. A copyright owner has the right to control the copying, adaptation, publishing, performance and broadcast of the work, and under what conditions this may be done. In addition to creating materials to

which copyright will apply, staff and students of colleges and universities are likely to use work that belongs to others extensively. Compliance with copyright law remains necessary in migration to the cloud.

In addition to any copyright protection, a database may be protected by the database right. The database right applies in the EU and is intended to protect and reward investment in the creation and arrangement of databases.

A patent protects the features and processes that make things work, allowing inventors to profit from their inventions. It gives the patent owner the right to prevent others from making, using, importing or selling the invention without permission.

For more detailed information on the law in this area, see the Copyright section of our website: [www.jisclegal.ac.uk/LegalAreas/CopyrightIPR.aspx](http://www.jisclegal.ac.uk/LegalAreas/CopyrightIPR.aspx)

Using a cloud provider for IT service provision raises particular IPR issues for institutions to consider prior to agreeing the terms of their cloud computing provision.

Two main issues arise:

- the cloud provider (i.e. a third party) may have access to data belonging to an institution
- the location of the data is not fixed

This has implications for an institution's IPR compliance.

### **Licence restrictions**

Software licences may be location specific and these will require review to ensure continued compliance when considering a cloud infrastructure service.

An institution will have contractually agreed with publishers via current educational resource licences (e.g. Copyright Licensing Agency Limited (CLA) licence) to safeguard resources. The licence agreement, for example, may state that only authorised persons e.g. staff and students may view the digital resource or storage of digital material may be restricted under the licence to local servers. There is a possibility of third party (i.e. cloud provider and their sub-contractors) access and the cloud is intrinsically not location specific. Contractual agreements with your resource

suppliers, on access and location, need to be reflected in your contract with your cloud provider via warranties. The cloud provider should provide assurances that best efforts will be made to prevent access by unlicensed users and to prevent any unauthorised usage of the licensed resources.

### **Creation of Content in the Cloud**

Where content is created in the cloud then whilst it may usually be possible to identify the creator and therefore the first copyright owner, it may be more difficult to identify where the material was created. This will not affect copyright protection per se, but may affect whether correct formalities have been followed in a particular jurisdiction, which in turn may affect ability to take court action if necessary.

### **Database Right**

If a database is recorded on a server in an EU member state then it is clear that a valid database right may apply, provided of course that the database meets the criteria outlined above for protection. However, research has raised the question of whether it is where the database is made or where it is recorded that is key and whether these are different places according to the legislation. This may potentially affect whether database right applies or not as there is no database right, for example, in the US. As there is no court decision on the interpretation, some uncertainty exists as to whether a database recorded on a non EU server will be protected by the database right. Further analysis on this is available in the QMUL paper Information Ownership in the Cloud, available at: [www.cloudlegal.ccls.qmul.ac.uk/index.html](http://www.cloudlegal.ccls.qmul.ac.uk/index.html). It is important to ensure that no residual database rights should be created for the cloud provider.

#### **Key Point**

Check current software and educational licence conditions to ensure that they are not breached by using a cloud service. Ensure that your contractual liabilities are reflected in the contract with your cloud provider.

## 2.6. Equality and Accessibility

As well as pedagogical reasons, the Equality Act 2010 places a legal obligation on institutions not to discriminate against students with disabilities; this obligation remains unchanged whether an institution is using a cloud provider or a location specific provider. Further information on the obligations under the Equality Act is available from the Equality Challenge Unit at [www.ecu.ac.uk/](http://www.ecu.ac.uk/) and from the Accessibility section of our website at:

[www.jisclegal.ac.uk/LegalAreas/AccessibilityLaw.aspx](http://www.jisclegal.ac.uk/LegalAreas/AccessibilityLaw.aspx)

### Key Point

When using a cloud provider, institutions remain responsible for provision of accessible services to students under equality legislation. They should check that the means of service provision will not adversely impact accessibility.

## 2.7. Contracts

As with other outsourced provision, a good service level agreement is essential. This should reflect an institution's requirements in areas such as data security, business continuity and disaster planning. It is essential that a reliable cloud provider is used whose data protection, and data security awareness is reflected in contract terms. Concerns on data locked in to one cloud provider have been expressed in particular with regard to newly established providers and institutions should perform pre contract due diligence to assess potential risks. The risks with regard to return of data in an insolvency or in a chain situation such as where your cloud provider has outsourced some of his provision e.g. data storage, should be addressed at the outset.

### Key Point

Institutions should ensure that the contract terms with cloud providers reflect their legal obligations, responsibilities and the level of risk they are prepared to handle.

### 3. Summary

While there are many potential benefits to cloud service provision, it is important to be aware of the legal challenges it presents and to ensure that careful consideration is given as to how continuing legal obligations and responsibilities are handled. As with all outsourced provision, it is important to be aware of these at the outset before agreeing any contract, as well as ensuring that those staff and students who will be implementing and then using the services are aware of the manner in which these obligations are to be met.



## About JISC Legal

JISC Legal, a JISC Advance service, provides guidance to prevent legal issues being a barrier to the development and adoption of new ICT within the education sector. It supports a wide range of staff within FE and HE, including managers, IT directors, administrators, and academics, with the aim to make best use of technology in developing institutional effectiveness, without legal issues becoming a barrier to appropriate use.

High quality, practical support is delivered through:

- Written publications e.g. Web 2.0 series, blanket copyright licences, e-repositories and the law
- Multimedia presentations, such as recorded webcasts on staying legal with web 2.0, and digital copyright. These offer the benefit of training delivered directly to lecturers and tutors at a time convenient for them
- Events at various locations around the country
- A short turnaround help desk. This enquiry service addresses problems specific to the enquirer. Common problems are then identified by the JISC legal staff and converted into helpful FAQs on the website
- Commissioned research projects and joint activities with other JISC Advance services

JISC Legal is a JISC Advance service. For more information on JISC Advance, please visit: [www.jiscadvance.ac.uk/](http://www.jiscadvance.ac.uk/)

JISC Legal is hosted by the University of Strathclyde, a charitable body, registered in Scotland, with registration number SC015263.

### “What can JISC Legal do for me?”

<b>Essentials</b>	Succinct guides to areas of law relevant to ICT use in further and higher education
<b>Overviews</b>	<b>More detailed guides to relevant areas of law</b>
<b>Publications</b>	A range of materials on specific issues
<b>Videos</b>	On important areas of law
<b>News</b>	Recent events relevant to ICT and law, with a focus on practical consequences
<b>Events</b>	A calendar of forthcoming events from JISC Legal
<b>Useful Links</b>	An access point to other relevant information providers
<b>Enquiries</b>	<b>A quick turnaround enquiry service, for those specific questions you may have</b>

### Keeping Up-to-date

Visit our website: [www.jisclegal.ac.uk](http://www.jisclegal.ac.uk)

Follow us on Twitter: [www.twitter.com/jisclegal](http://www.twitter.com/jisclegal)

Tune-in via Vimeo: [www.vimeo.com/jisclegal](http://www.vimeo.com/jisclegal)

Or Subscribe to our free, monthly email newsletter: [www.jisclegal.ac.uk/newsletter](http://www.jisclegal.ac.uk/newsletter)