

August  
2011

## User Guide: Cloud Computing Contracts, SLAs and Terms & Conditions of Use

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



### What's in this Guide?

This is a practical guide to the terms and conditions commonly found in cloud computing service provision contracts and agreements.

It is designed to assist you in understanding the division of rights and responsibilities between the provider and the user of a cloud computing service, and to allow you to make an informed judgement as to the legal risk.

This guide is part of the JISC Legal Cloud Computing toolkit. Information on how to access the full toolkit is at the end.

### Key Points

- Adopting cloud computing services does not change an institution's legal duties, only the means by which the institution will comply.
- The Cloud Computing Contract and Service Level Agreement are essential steps in implementing a successful cloud computing solution.
- Particular issues to be considered are clauses relating to jurisdiction, security of data and intellectual property rights.

## Contents

<b>1. Introduction.....</b>	<b>2</b>
<b>2. Cloud Computing Contracts.....</b>	<b>3</b>
2.1. Data Protection.....	4
2.2. Intellectual Property Rights.....	6
2.3. Freedom of Information Obligations.....	7
2.4. Legal Compliance.....	8
2.5. Law Enforcement and Loss of Control.....	8
2.6. Licensing.....	8
2.7. Confidentiality.....	9
2.8. Monitoring by Cloud Provider.....	9
2.9. Law and Jurisdiction.....	10
2.10. Data Retention Schedules.....	11
2.11. Subcontracting.....	11
2.12. Acceptable Use Policy.....	11
2.13. Warranties.....	12
2.14. Indemnities.....	12
2.15. Exclusions and Limitations of Liability.....	13
2.16. Change of Service by Cloud Provider.....	15
2.17. Termination.....	15
<b>3. Service Level Agreement.....</b>	<b>16</b>
<b>4. Summary.....</b>	<b>17</b>

---

### 1. Introduction

This practical guide outlines the specific risks associated with contractual arrangements for procuring and implementing cloud computing solutions. It is aimed at any educational professional involved in the process of setting up or managing contracts for cloud computing solutions. It will be specifically useful to project and risk managers, contract managers, IT professionals, and procurement managers in FE and HE.

Getting the contract terms right between FE and HE institutions and cloud providers is essential for the successful implementation of cloud computing. The contract terms and conditions should set out responsibilities, service expectations, financial arrangements and what happens if things go wrong. In addition to the usual contractual considerations with any commercial agreement with a third party, cloud

computing raises a number of legal considerations specific to the nature of internet based service delivery.

## 2. Cloud Computing Contracts

The most important factor at the contract stage of any cloud computing project is to ensure that the cloud provider will take reasonable steps to meet the institution's existing legal duties while they are providing the service. The main legal considerations at this stage are data protection, data security and jurisdiction. There are also some intellectual property matters to manage and general contract law considerations.

The contract terms and conditions between institutions and cloud providers set out the division of responsibility for both parties at the organisational and operational level. Cloud computing contracts may set out Service Level Agreements (SLAs), any licence agreements, security schedules, clauses on rights and responsibilities and processes to be activated on non-performance or breach of contract.

Cloud computing contracts can vary in format and wording depending on the cloud provider and type of solution the institution is procuring. For all cloud computing contracts it is good practice to ensure that legal areas are dealt with to your satisfaction and to seek legal guidance where appropriate. Areas that are dealt with in more detail below include:

- the obligation to comply with data protection legislation
- appropriate management of intellectual property rights
- maintaining the capability to comply with freedom of information legislation obligations
- law enforcement obligations - access to cloud data
- confidentiality of information
- appropriate licensing of resources
- monitoring of users and security of data
- regulating acceptable use of IT systems - safeguarding users

## 2.1. Data Protection

The Data Protection Act 1998 (DPA) governs how the personal data of individuals is processed. Whether outsourcing processing of personal data to a cloud provider or processing personal data internally, as data controllers, institutions are required to ensure that all processing of personal data that they are responsible for adheres to the eight data protection principles. Whilst compliance with all the data protection principles is necessary it is the seventh principle relating to security of data and the eighth principle relating to the geographical jurisdiction of where data is stored which are most problematic for UK institutions using a cloud provider. More information about the application of the data protection principles, which are contained in a schedule to the DPA, is available on the Information Commissioner's Office (ICO) website at:

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

### 2.1.1. Data Security

The seventh data protection principle requires an institution to ensure that personal data relating to its staff, learners and others remains secure, including protecting such data from accidental loss, damage and destruction. Where an institution uses a third party, in this case a cloud provider, to process personal data on its behalf it will be responsible for what the third party does with the data. This means that an institution could be liable where data stored using a cloud provider is lost or destroyed.

The institution has an obligation to ensure that its cloud provider has adequate measures in place to protect personal data securely against unauthorised or unlawful processing and against accidental loss, destruction and damage. The institution can manage these requirements by including a security schedule within the contract with its cloud provider which outlines how they handle personal data, including:

- how the institution's data is separated from other organisations' data
- restrictions on the use of personal data
- responses to security breaches
- reactions to UK DPA requirements
- use of security measures such as encryption

Institutions may want to ensure that the contract with their cloud provider contains a suitable indemnity in relation to any claim from an individual (data subject) as a result of unlawful processing (including breach of security) by the cloud provider.

Insisting on industry standard security requirements within the cloud service contract will also reduce the likelihood or impact of the institution facing a third party claim under contract law for a breach of security where it has agreed in a contract with a third party to ensure the security of data. Similarly, it may reduce the likelihood of a claim in negligence from a third party alleging that the institution failed to take the security precautions reasonably expected.

### 2.1.2. Geographical Location of Data

Cloud providers are likely to store and move data around multiple servers situated in a number of jurisdictions which may very likely be outside the European Economic Area (EEA). The DPA restricts the transfer of personal data to countries within the EEA (the eighth data protection principle). The transfer of personal data outside the EEA is not permitted unless the country has an adequate level of protection for the individual in relation to the processing of personal data.

The institution may be concerned about the security of personal data stored by a cloud provider outside the EEA. An institution as data controller will remain responsible for the adequate protection of the personal data of their staff, learners and others and will need to find out where the cloud provider is processing data in order to assess how to proceed.

To maintain compliance with the DPA, the institution should consider using a cloud provider in a country already assessed by the European Commission as having adequate protection, or a US provider who has signed up to the Safe Harbor Regulations (this can be checked on the US Trade Information Center - Export.gov website:

[safeharbor.export.gov/list.aspx](https://safeharbor.export.gov/list.aspx) or use European Commission approved contract terms with its cloud provider. Further information regarding transfer of data abroad can be found on the ICO website: [www.ico.gov.uk/](http://www.ico.gov.uk/).

When contracting with a cloud provider, it is good practice, as part of the contract, to ensure the institution has a warranty or a legal contractual assurance with respect to the geographical location of the institution's stored or archived data. The institution should also consider adopting a reporting or audit mechanism to monitor compliance with this requirement. Some major cloud providers offer a number of "regional zones" in which a customer may be assured the data will remain. For example, Amazon's sign-up process includes a choice of storage domains:

[aws.amazon.com/s3/faqs/#Where\\_is\\_my\\_data\\_stored](https://aws.amazon.com/s3/faqs/#Where_is_my_data_stored) and Amazon's AWS Customer Agreement (updated in 2011) includes an undertaking not to transfer content from the selected region without notification, unless required to comply with the law or requests from governmental entities: [aws.amazon.com/agreement/](https://aws.amazon.com/agreement/)

Fundamentally the data protection principles apply to the processing of personal data irrespective of the geographical location chosen by the institution or the cloud provider. The legal contract with the cloud provider is the means by which the institution ensures that its legal obligations continue to be fulfilled.

## 2.2. Intellectual Property Rights

An arrangement with a cloud provider how intellectual property rights are to be handled is an important aspect to get right from the outset.

In contrast to concerns often expressed regarding cloud services, an analysis of cloud provider's standard terms and conditions conducted by the Queen Mary University of London School of Law indicates that cloud providers do not normally assert ownership of the intellectual property rights in content and data uploaded by their users (Queen Mary University of London School of Law Legal Studies Research Paper No. 63/2010 Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services: [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1662374#](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374#))

However, the nature of the cloud means that information is constantly being added and removed or modified, and new information generated, therefore, it is important to review the cloud provider's terms and conditions and ensure that the contract is clear where ownership of this new data lies. It is essential to state in the contract that all data will continue to be owned by the institution and to ensure that any residual database rights are owned by the institution. For example, institutions will want to

retain copyright in literary works (teaching and research materials), database rights, and design rights in software.

When several institutions are working together on a private cloud, they may decide to draw up a consortium agreement outlining the terms and conditions of the arrangements for collaborative working between institutions. This means that should there be a change in institutional structures or personnel, the collaborative working arrangements remain clearly defined. The consortium agreement should also set out how intellectual property rights are assigned for new materials created as part of the private cloud (for example, a shared guidance manual, or a data centre used for data mining with a shared centre licence), and specify how metadata will be tagged.

Cloud providers, although not asserting intellectual property rights, frequently include in their contract terms and conditions a term that their customer (the institution) grants the provider a compulsory licence to republish some or all of the customer's data for the purpose of provision of the service. The institution will want to ensure that the extent of any licence is:

- limited to what is necessary for the provision of the cloud computing service.
- compatible with the institution's obligations under the DPA to process data fairly and lawfully and for limited stated purposes.
- compatible with its obligations to third parties.

### 2.3. Freedom of Information Obligations

Freedom of Information (FOI) legislation gives individuals a right of access to information held by the institution. The legislation covers all records and information held whether digital or print, current or archived. Even though the information is stored in the cloud, an institution will still be deemed to be holding it for the purposes of FOI.

It is important for the institution to address in the contract with its cloud provider how timely access to information is facilitated. It is also important to ensure that outages and failures at the cloud provider's end do not prevent the institution from fulfilling its legal obligations to respond to FOI requests within twenty working days.

## 2.4. Legal Compliance

The institution should have in place a take down policy for its internal and external published content in the event of being notified of material that breaks criminal or civil law. The institution should assess whether the cloud provider can give assurances that information can be taken down without delay from websites or other accessible locations on the instruction of the institution's IT director. The institution needs to ensure in the contract with its cloud provider that there are policies and procedures which will enable the institution to comply with its investigation and take down policy.

## 2.5. Law Enforcement and Loss of Control

The Regulation of Investigatory Powers Act 2000 (RIPA) governs disclosure of information by the institution to law enforcement agencies. These obligations will remain for FE and HE institutions irrespective of the type of infrastructure being used, cloud or otherwise. The contract with the cloud provider is the means by which the institution maintains control over its data and records and which enables its own compliance with law enforcement obligations.

## 2.6. Licensing

An institution will have contractually agreed with publishers via current educational licences (e.g. The Copyright Licensing Agency Limited (CLA)) to safeguard resources. The licence agreement 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 licence to local servers. When using cloud computing services there is the possibility of third party access e.g. by the cloud provider or their subcontractors and the location of data may not be specific. Contractual agreements with the resource suppliers regarding location and access need to be reflected in the contract with your cloud provider. The institution may require assurances from the cloud provider in respect of geographical location of data (see section 2.1.3 hereof) and that best efforts will be made by the provider to prevent access by unlicensed users and to prevent any unauthorised usage of the licensed resources.

## 2.7. Confidentiality

There are many occasions when information is required to be kept confidential by administration staff or researchers at an institution. This will include handling personal health data, some types of employment related data, and management related data that may be sensitive commercially. Prior to entering into a cloud service agreement, senior managers will want the proposed systems to be tested to ensure that confidential data can be processed without being compromised and will also require to assess whether the cloud is an appropriate place to store and work with certain information where confidentiality is critical.

The processes in place for protecting confidentiality should include outlining confidentiality provisions in the contract. The standard terms and conditions of cloud providers vary in the degree to which they undertake to maintain the confidentiality of customer's data. In fact, some cloud providers state that they have no duty of confidentiality regarding customer data and place responsibility for confidentiality on the institution, for example, via encryption. Therefore, it is desirable to state clearly in the contract terms what obligations of confidentiality are owed between the parties.

## 2.8. Monitoring by Cloud Provider

Institutions may not want their use of the cloud service to be monitored by their cloud provider either due to concerns regarding the outcome of such monitoring or because it may disclose the institution's confidential data to the cloud provider. Cloud providers have different policies with respect to monitoring, for example:

- monitoring the nature and pattern of use (such as bandwidth consumption)
- monitoring use specifically for the purpose of ensuring a good quality service provision
- for statistical analysis
- for enforcing their Acceptable Use Policy (AUP)

The institution will need to examine the contract details to ensure that the terms are clear with respect to the level of monitoring carried out and that the terms are consistent with their own requirements.

## 2.9. Law and Jurisdiction

The nature of the cloud is such that it is likely that more than one legal jurisdiction will be involved in relation to any particular external cloud service. For example, relevant jurisdictions are likely to include the UK (where the institution is based) and the countries where the cloud provider, its servers and any subcontractors reside.

The laws governing which country's laws apply to a particular issue and which country's courts will hear a particular dispute can be complex. The resolution may vary according to the area of law and the jurisdiction in which the question arises. However, some general observations are possible.

A cloud provider will normally specify within its contract terms that the contract is governed by the laws of a specific country and that disputes will be heard in that country's courts. Usually this will refer to the jurisdiction in which the cloud provider has its principal place of business, but occasionally it may be the legal system where the customer is based. The law typically places few restrictions on this type of contractual clause, except some controls on electing a totally irrelevant jurisdiction, and more stringent controls in relation to consumer (non-business) contracts.

In the event of a dispute the institution, if possible, will want to avoid having to enforce contractual terms in an overseas jurisdiction, under foreign law, or having to defend an action in an overseas jurisdiction and under foreign law. Institutions may therefore have to consider the possible additional costs if the cloud provider chosen applies a foreign choice of law and jurisdiction clause, versus the benefits of that particular service.

For further analysis of the laws and jurisdiction applicable in cloud computing contracts refer to the [Terms of Service Analysis for Cloud Providers](#), Legal Studies Research Paper No. 63/2010, published by Queen Mary University of London School of Law.

## 2.10. Data Retention Schedules

The institution is likely to have committed to and have in place practices and procedures for records handling to enable disposal and retention of data as required by its legal obligations. How these retention schedules are complied with when the data is hosted and processed in the cloud needs to be clarified in the contract with the cloud provider.

## 2.11. Subcontracting

It is important to determine whether third parties will have access to data, for example, to what extent elements of the cloud service are subcontracted by the cloud provider to third parties. If subcontracting takes place, the institution should ensure that the terms of the contract with the cloud provider reflect the institution's security requirements.

## 2.12. Acceptable Use Policy

Cloud providers are broadly similar with respect to the rules they impose on how an institution may use their services. Such rules will frequently be embodied in an Acceptable Use Policy (AUP) which highlights the cloud provider's need to exclude liability arising from the actions of its customers. An AUP will normally outline activities deemed to be improper or outright illegal uses of the cloud service. Examples may include bulk unsolicited commercial email (spam), fraud, gambling, hacking into other systems or the hosting of content that is obscene, defamatory, or which may promote discrimination or incite hatred. The institution should review the cloud provider's AUP to ensure that the institution can comply and it may be worth comparing the terms with those contained in the institution's own AUP for users of its IT systems and infrastructure. The types of activities which are not considered acceptable are likely to be similar.

## 2.13. Warranties

In common with any outsourced service, the institution should consider any warranty it would expect to receive from its cloud provider in relation to the performance of the cloud services. It should examine the extent of any warranties provided in the cloud provider's terms and conditions accordingly.

The research into standard terms and conditions of cloud providers conducted by the Queen Mary University London School of Law indicated that every cloud provider surveyed went to great lengths to deny that any warranty existed in respect of performance of the services. US providers were particularly comprehensive with respect to excluding warranties. The result of this research highlights that any warranty required by the institution would need to be negotiated with the cloud provider.

## 2.14. Indemnities

### 2.14.1. Institution

As with any outsourced service, the cloud provider's terms and conditions will normally incorporate indemnification clauses. These require the institution to indemnify (undertake to compensate for loss) the cloud provider against any claim arising from the institution's use of the service and this is the case even where the service provided is free. The institution should review the indemnification provisions as they would when procuring any service.

### 2.14.2. Cloud Provider

Some cloud providers undertake to indemnify (compensate for loss) the customer in certain circumstances. Google, for example, (for Google Apps Premier [www.google.com/apps/intl/en-GB/terms/premier\\_terms.html](http://www.google.com/apps/intl/en-GB/terms/premier_terms.html)) will indemnify the institution against any liability arising from a third party claim that Google's technology used to provide the cloud service infringes third party intellectual property rights.

Institutions should ensure that the contract with their cloud provider contains a suitable indemnity in relation to any claim from an individual (data subject) as a result of unlawful processing (including breach of security) by the cloud provider.

## 2.15. Exclusions and Limitations of Liability

The institution should scrutinise the limitations of liability in the contract with its cloud provider as they would do in any case when outsourcing services. It is worth bearing in mind that limitations of liability may be buried within other provisions of the contract, for example, in the force majeure provisions or within a separate Service Level Agreement. (Force majeure is a term that effectively means unexpected events that prevent someone from doing what they had agreed to do - see section 2.15.3 below.)

### 2.15.1. Direct Damages

The institution's cloud provider may include, in their standard contract terms and conditions, an exclusion for some categories of direct damages. Such terms are designed to limit the cloud provider's liability.

The research carried out by Queen Mary University London School of Law found that cloud providers based in the US tended to seek to deny liability for direct damages as far as possible while European based cloud providers were less overt about seeking to exclude direct liability, presumably on the basis that in most European legal systems it is difficult to do so. This difference in approach may be a point for the institution to consider in its selection of cloud provider.

The limitation of liability provisions should be carefully examined to determine the extent of any exclusion of liability for direct damages. For example, in the case where a cloud provider loses data, the institution may be able to claim for direct losses such as the cost of reconstituting data or the cost of notification. This will not be the case if the cloud provider has included an absolute exclusion of liability for loss of data in the contract.

In assessing the cloud provider's liability for direct damages, the institution should also review the terms of the Service Level Agreement (SLA) to determine whether the provisions of the SLA state that the performance rebates provided in the SLA are the sole and exclusive remedy for failure in the service provision. In cases where the SLA is framed in such terms this would effectively prevent the institution from claiming for any other direct damages arising from loss of service which exceed the level of rebate but are within the overall cap on liability in the contract (SLAs are dealt with in more detail in section 3 below.)

### 2.15.2. Indirect Damages

It is standard practice for service providers to exclude liability for indirect or consequential loss, for example, loss of profits. The case is no different for providers of cloud services. However, in reviewing the contract terms, the institution should be wary that the cloud provider does not include loss of data in its description of indirect losses.

### 2.15.3. Force Majeure

Force majeure is a boilerplate clause normally included in service contracts to exclude liability for losses arising from circumstances outside the reasonable control of the service provider. It often includes examples such as natural disaster, governmental action, act of war or terrorism or, in the case of cloud computing services, interruption to the internet.

In the case where the institution is aware that elements of the cloud service will be or may be subcontracted to a third party the institution should determine whether the force majeure provision in the contract with its cloud provider excludes liability resulting from any failure of a subcontractor. While it may be acceptable that liability is excluded where the subcontractor suffers a force majeure event. it may not be acceptable to the institution that it has no means of recourse against its cloud provider where failure in the service results from the actions of a subcontractor, in particular, where the cloud provider takes no action to rectify the situation and has not carried out any audit or monitoring of its subcontractor.

### 2.15.4. Cap on Direct Loss

It is typical, in the terms and conditions of cloud providers, to include an overall cap on the extent of any damages for which the cloud provider will be liable which is related to the value of the contract. This can be expressed, for example, as the value of the lifetime of the contract or as the amount of the fees paid by the institution in the twelve months prior to the event giving rise to the liability.

In cases where a cloud provider limits its legal responsibility to a specific amount, the figure stated will depend on the nature of the cloud service and the type of users for such service.

In assessing whether the cap on liability proposed by the cloud provider is acceptable, the institution should use similar criteria as it would use in the procurement process for any other outsourced service.

## 2.16. Change of Service by Cloud Provider

In comparison with traditional software licensing, where an institution has no obligation to upgrade to a new version of software but may find that the old version is no longer supported, in cloud computing the cloud provider may expect to migrate all its customers to the latest version. This explains why standard contracts containing a provision where changes require written agreement of both parties tend to be the exception rather than the rule.

An institution however, may be cautious of its cloud provider having a unilateral right to make changes to the service terms and conditions without notice which places an onus on the institution to review the terms and conditions as hosted on the cloud provider's website on a regular basis to check whether there have been any changes.

The institution may opt for a middle ground with its cloud provider whereby different classes of change are handled differently. For example it may be appropriate to allow the cloud provider to make changes to avoid intellectual property infringement or service changes that do not impact on functionality without notice. Likewise it may be appropriate to require notice and possibly an option to terminate the contract in the case of a material change in the service which negatively impacts on the institution.



## 2.17. Termination

The contract terms and conditions for cloud services will usually specify the initial duration of the contract, its renewal period and the steps to be taken by either party to terminate the contract. It is not unusual for the contract to continue indefinitely subject to payment of service fees and unless terminated by either party. The institution will expect the contract to be clear with respect to the circumstances under which either party may terminate the contract. An important issue for institutions is what happens to their data following the end of the relationship with their cloud provider.

### 2.17.1. Possession of Data on Termination

The institution will want to ensure that they reserve the right to have data returned on termination of the contract and that the contract is specific about the format in which data is to be returned. The terms should be clear on the length of time during which data will be preserved by the cloud provider in order for the institution to retrieve it and details of charges or conditions, if any, in respect of such retrieval.

### 2.17.2. Deletion of Data

The contract should outline the procedure agreed between the parties with respect to deletion of data. The institution will want to know whether the cloud provider will delete their data on termination of the contract. It is likely that in order for the institution to ensure compliance with its legal obligations with respect to data and to preserve confidentiality the institution will want all copies of data in the possession of the cloud provider deleted after it has exercised its rights to have data returned.

## 3. Service Level Agreement

Although many cloud providers may seek to exclude or limit liability for performance of the service some providers will outline in a separate Service Level Agreement (SLA) a service performance target that it will aim to meet and provide a mechanism for compensating the institution for failure to meet such target.

The compensation to the institution will usually be in the form of a services credit providing the institution with a rebate against billing for future services. The institution will want to ensure that the level of performance rebate is sufficient to compensate the institution and incentivise the cloud provider.

The institution will want to examine carefully the period within which service levels are measured in particular with respect to the definition of “availability”. For example where a cloud provider commits to 99.9% service availability then the actual service downtime will be significantly less if the 0.1% downtime is measured over a period of twelve months rather than being measured over one month.

The SLA will usually include a list of exclusions where the performance targets and consequently performance rebates will not apply including such causes of downtime as scheduled maintenance or any circumstances outside the cloud provider’s immediate control, such as routing or traffic issues affecting internet links.

The SLA will often be expressed as an exhaustive or exclusive remedy for failure to provide the service. If performance rebates detailed in the SLA are stated to be the sole remedy available for failure to perform the services then the institution may be unable to terminate the contract for material breach where the breach is failure to provide the agreed service/meet service levels agreed and may be restricted from pursuing the cloud provider for any direct damages over and above the performance rebate. The SLA may also define the support available from the cloud provider with respect to the provision of its services.

#### 4. Summary

For institutions the legal obligations will largely remain unchanged in the cloud environment. However the means by which an institution ensures that its duties are met have to be adapted to fit any new service delivery model using cloud computing solutions. The contract is a critical step to achieving a successful and legally compliant relationship with the cloud provider. The legal issues this raises are similar to any contractual issues that arise when outsourcing information services to a third party. One particular issue that arises when using an internet hosted service provision is jurisdiction and the institution’s obligations in terms of principle eight of the Data Protection Act 1998. Ensuring security of data held in the cloud is also a key factor. Thinking about who will own what with regard to intellectual property rights is also important to set out in the contract. Finally, as with all commercial contracts, it will be necessary to obtain appropriate legal advice and carry out proper risk assessments when choosing your cloud computing solution.



## 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)