Introduction

This pack contains articles dealing with four key legal issues of relevance for companies with an online presence.

Website terms and conditions

A website presence is a fundamental tool for an expanding business, whether just for advertising or for providing an online sales channel.

An alluring website is the first step, but legal issues governing the operation of a website and sales from it cannot be overlooked. Appropriate terms and conditions are not only an essential legal requirement, but a vital means of gaining customer confidence and building a credible brand.

Be aware of the legal regime

Any organisation advertising or trading on the internet, whether a fledgling business or an established operation expanding its e-commerce presence, is subject to a panoply of laws. Most of these already apply to the traditional retailer, but there are many additional provisions which apply to online operators and others trading at a distance which can trip up the unwary trader and create avoidable problems.

Governments of EU member states decided during the infancy of the internet that appropriate EU-wide legal provisions should be implemented to foster confidence in internet commerce and to gain consumers’ trust when they are not dealing face-to-face with suppliers.

“Why can’t I just use my usual business terms and conditions on my website?”

A canny supplier may be able to recycle his normal trading terms and conditions for online use. Even well-drafted ‘offline’ terms and conditions will need certain changes and additions to bring them into line with the rules for website contracts.

All sole traders, partnerships, companies and other legal entities must disclose certain key details, such as postal or trading addresses, email address(es), VAT registration number, a company’s country of registration and its registered number. There are special rules where the supplier of goods or services is a member of a regulated profession or industry or a member of a trade body.

Accordingly, laws specifically regulating e-commerce will mean significant ‘topping and tailing’ of traditional terms and conditions to ensure legal compliance (see below).

“What do I need in my website terms and conditions?”

There are various laws which specifically affect internet trading. As well as the normal provisions in sales contracts relating to the price and payment provisions, restrictions of the supplier’s liability and other standard ‘boilerplate’ clauses, there are special requirements for e-commerce contracts.
For example, the customer must be told whether the price includes VAT and delivery costs and how and exactly when the online contract is made. A prudent trader must ensure that the ‘offer’ and ‘acceptance’ stages of a binding contract are carefully managed. The supplier needs to ensure that he is the one confirming acceptance of the contract, so that he is not in breach of that contract if he has insufficient stock or has inadvertently advertised the product at the wrong price.

It is also necessary, under the ‘Distance Selling Regulations’, to notify consumers (someone not buying in the course of a business) of their right to cancel an online contract and obtain a full refund of any money paid, even if the goods are not faulty. There are precise rules on cancellation and the required notices, but consumers must be told that they have at least 7 working days (excluding weekends and bank holidays) after delivery to return the goods, even if they are not defective. There are exceptions for certain goods, such as bespoke or perishable items.

As well as addressing the supply of goods and/or services, the terms and conditions must also deal with the ownership, use and availability of the website itself, prohibit spamming and unsuitable postings to interactive sites and assert intellectual property rights.

Anyone collecting customer names and other personal information online must comply with certain procedures concerning the collection, storage, use and transfer of that data under data protection law. A website privacy policy is, therefore, a must.

“But I’ve already got website terms and conditions”

No matter how good the website terms and conditions may be, if insufficient steps have been taken to draw them to customers’ attention before the contract is made, they will not be ‘incorporated’ into the contract with the customer and they will not be legally binding. You must therefore expressly draw your terms and conditions to the customer’s attention before the contract is concluded.

Lyndsay Gough is an IT, e-commerce and intellectual property law specialist at Keystone Law. Before joining Keystone, Lyndsay was at City firm Richards Butler before joining Keystone in 2003.

E: lyndsay.gough@keystonelaw.co.uk
Online advertising and sales copy

So you want to start advertising your goods or services to increase sales. There is no question that the web is the fastest growing medium and lets you reach a very targeted audience. It also allows you to monitor the success of your advert. There has been a lot written about how to advertise and how to use pay per click, but what should you actually say (and not say!) in your advert? Here are some simple rules to help you keep the right side of the law when writing your own website copy.

What should I say about my business?

You do not have a free rein in relation to the content or arrangement of your own websites. Certain details concerning the business must be provided on the site in an easily accessible manner. You must specify your business’s trading name and the name of any company it trades through, the names of the directors (or a statement that such names are available for inspection at your registered office), the address of your registered office and your company registration and VAT numbers. You must also make it clear where you can be contacted, by phone (legally you do not have to give a phone number, but can you afford not to?), email, fax etc. and a correspondence address should also be specified if it’s different to that of your registered office. It is a criminal offence to miss out these basic details.

What should I say about my goods or services?

The Trade Description Act will apply to what you say on your website, just as it would to your paper adverts, as will the Consumer Protection from Unfair Trading Regulations (applies if you are selling to consumers). In general terms, traders must not make commercial communications to consumers which are:

- actually misleading (by act or omission);
- aggressive, i.e., by suggesting that if you do not take this offer up NOW, something terrible is going to happen;
- accurate; it may well be the best product in its class, but to say so can lead to accusations that you have incorrectly described the product. One common way round this is to refer to survey results or an independent publication, e.g., ‘eight out of ten people said it is the best product in its class’, or ‘according to “What Product Magazine”, it is the best product in its class’. Try and stick to the facts, and steer clear of claims you cannot prove; and
- complete; you must also give the consumer sufficient information about the product, to make an ‘informed transactional decision’, so that they know the delivery times and the life of the product, or whether they need to buy additional batteries for it. An omission can therefore be just as serious as an inaccurate description.

You will need to ensure that all of this information is either in one place, or can be read together, relatively easily, using links or references.
What promises can I make?

If a buyer of your product/service argues that a statement that appeared on your website which induced them to buy your product and the statement is subsequently found to be untrue, you're in trouble. Such statements are a representation by you about the product or service and they need to be accurate. Performance indicators often cause the biggest problem. Saying that something will work for ten times longer than its competitor, and then it only works for four times as long, leaves you open to a misrepresentation action and you may be held liable to compensate the buyer for the loss. If the information comes from the manufacturer, you can still be liable if you publish it on the website, because you have assumed responsibility for it by including it within your product's description. Although you would be able to reclaim your loss from the manufacturer, you may not want to have this problem. You might consider instead linking to the manufacturer's site or providing the information in a way that makes it very clear who is making the claim.

Can I offer guidance and advice?

If you recommend a way of using your product or service (e.g., give directions, installation instructions etc.) or a person who can install or repair that product, then you will have to stand behind that recommendation. You might therefore say that all your technicians exceed some specification of quality or training. If that is not correct, then you may be liable for any loss suffered by the consumer or buyer (though do note that claiming to have qualifications in this way is often less risky than claiming that the product will perform in a certain way).

What about ‘special industries’?

There are a number of special industries that are subject to a higher level of restrictions in their advertising materials. These include such areas as financial services, and food and drink products, tobacco and alcohol. If you are dealing in these products or services you need to check what further restrictions apply.

Do I really have to comply with these requirements?

Yes! Trading Standards are very hot on compliance with the law and have the power to take down your website. Consumers and buyers are often clued up on their rights and won’t stand for breaches. They may sue you and win or report you to Trading Standards. Furthermore, from March 2011 the Advertising Standards Authority’s (ASA) digital remit will be extended to cover marketing communications made on websites by businesses, sole traders, organisations and companies. As well as its existing sanctions, the ASA will be able to name and shame offenders, usually as a result of complaints received. This means that if you may need to review your website to ensure that its marketing content complies with the Committee of Advertising Practice (CAP) Code. You can find a useful document about the Code, its new wider application and sanctions at www.asa.org.uk, the ASA’s website.

Cases of fraud or obtaining property by deception attract serious civil and criminal penalties, respectively. Lastly, and most importantly, in this day and age of rapid information transmission and so much choice, your reputation matters. It is no wonder that sellers through eBay choose to look after their buyers (on the whole) very well; they don’t want buyers to shop elsewhere!
Disclaimers

All of the above can be quite daunting, especially if all you want to do is convey your message through your website in the way you think best. You may find using a disclaimer helpful in this type of situation. A properly-worded disclaimer makes it clear that anything you say on your website is not meant to form or be part of a contract between you and your customers, and that your customers should themselves evaluate the products and/or service you recommend. It isn’t a perfect safety net (the courts will still look at whether you influence the customer’s buying decision in a way you should not), but it does give you some contractual protection. It is not possible to offer a precedent disclaimer because, as a matter of law, there are some areas for which you cannot disclaim liability and, more importantly, what you disclaim needs to relate to what you say in the first place.

Jill Benbow is a commercial litigator with significant experience acting on commercial property matters. She was previously a partner and head of litigation at Fraser Brown, and has handled a wide range of disputes for individuals, as well as companies of all sizes.

E: jill.benbow@keystonelaw.co.uk
Privacy Policy

The collection, organisation and distribution of personal and other confidential data is a fundamental concern, which, if ignored, can cause both legal and administrative headaches for any business.

Legally, the regime differs depending on the country in which the business resides, but in the UK the principal legislation is the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the Regulations). Compliance is monitored via the Information Commissioners Office and it provides useful and detailed guidance on their website: www.ico.gov.uk. The ICO also plans to release a formal code of practice in May 2010.

While the legal burden is not insignificant, the use of data protection requests under the DPA has increased markedly over the past few years and along with it the administrative burden of compliance. Consequently, businesses are also finding it increasingly important to know what their obligations are and to put resources in place to meet them administratively. A well-drafted privacy policy allows them to do both.

Are privacy policies required by law?

While there is no legal requirement to have a privacy policy as such, in order to comply with the relevant legislation there are several hurdles over which any site using personal data must pass. Therefore it is strongly advisable to have one.

Consent

Consent is not required where processing is necessary for the performance of a contract with the data subject, but unfortunately ‘necessary’ is a potentially grey area and so obtaining consent is now deemed best practice.

Consent of the data subject must be ‘freely given, specific and informed’. Although it can be implied in the UK, a well-drafted privacy policy will set out when consent is deemed to be given, and how to avoid doing so, thereby meeting the first element. Defining the specific use of the content meets the latter parts.

Also, according to the ICO, consent must be a positive act, a pre-ticked box is not sufficient and, importantly, they must be able not to consent.

In order to use ‘Cookies’ or forms of direct marketing, consent must be given and so their use must also be carefully spelled out in the privacy policy.

For any of this to be meaningful, it is essential that the data subject can access the privacy policy and locating a link to it as close to the “Submit”, “Agree” or “Accept” buttons is vital.

Processing

‘Processing’ is a term that is often defined in privacy policies in the widest possible terms, to include distribution and disclosure, as well as the more obvious collection, manipulation and storage facets of processing. Companies using personal data should ensure that they actually have the right to ‘process’ the data in the manner they wish, rather than simply assume that they can.
**Personal data**

‘Personal data’ comprises not only names and addresses, but personal measurements by and on any scale, any form of further contact details, medical records, historic data on behaviour and a myriad of other facets of human existence and activity. In order to be able to use such data successfully and, importantly, without challenge, they must be defined and included in the privacy policy.

**Marketing benefits**

A privacy policy can also help a company establish credibility and reassure users that the business concerned has taken steps to ensure their data is protected. At one stage this would have been a differentiator, but now such probity is assumed and any site collecting data without a privacy policy is likely to be viewed with suspicion and avoided.

**Penalties**

Breaches of the DPA, such as failure to notify the Information Commissioner of any proposed processing, can lead to criminal sanctions. These include up to a £5,000 fine on summary conviction, or an unlimited fine if convicted on indictment.

Furthermore, directors and other company officers may assume personal liability.

In practice, the ICO has tended to adopt a collaborative approach to rectify breaches before commencing enforcement, but the penalties remain and coupled with the cost of negative publicity, any company using personal data would be well advised to invest in a privacy policy to protect itself.

**International issues**

**Establishment**

The DPA applies to data controllers who are ‘established’ in the UK, which includes UK registered companies, any organisation maintaining an office or branch in the UK, or individuals who are ordinarily resident in the UK.

Therefore, overseas companies and even foreign nationals so ‘established’ will need to comply.

**Processing**

However, jurisdiction does not end there. While, mere transit is excluded, even data controllers ‘established’ outside of the UK are required to comply if they use equipment to process the data which is located here. Therefore, even a non-UK company with no ‘presence’ in the UK other than via a data storage agreement with a server farm in (for example) Reading, will need to comply. Similarly, if an overseas company outsources data analysis to a UK company, the regime will also apply.

**Multi-jurisdictional compliance**

Clearly, this approach to ‘establishment’ and ‘processing’ may mean that a company has data protection obligations not only in the UK, but potentially in any other country with internet access as well.

There is no principle of ‘dominant compliance’ or law of choice, as you might have under contract law. The relevant data controller will need to ensure that he or she is compliant in all jurisdictions in which the business is established or processes.
While the EU Data Protection Directive is the basis on which all the EU member states have legislated in this area, it has not been implemented uniformly and the obligations on the data controller vary between member states. Data controllers are advised to verify each jurisdiction’s requirements individually.

Further considerations

Optional data
Care should be taken to indicate where data is optional, since there is an obligation not to collect data which is excessive with regard to the purpose for which it is collected. For instance, while salary details may be useful for, say, school fundraising purposes, a user enquiring about joining an alumni association should not be obliged to provide such information.

Uncommon methods and purposes
With the rise of more innovative businesses and modes of communication, the methods by which data is collected and purposes for which it is used are developing at a startling rate. The meteoric rise of the iPhone and user-location/data-related ‘apps’ is a prime example. Businesses need to ensure that their unique approach doesn’t compromise their ability to comply with the legislation.

Sensitive personal data
The DPA requires ‘explicit consent’ to the processing of certain sensitive personal data such as that relating to racial or ethnic origin, political or religious belief.

Breach of these provisions is considered particularly serious, therefore any business which suspects it may wish to process such data should seek specific professional legal advice.

Conclusion

Since Keystone Law advises many entrepreneurs, we have seen the increasingly anachronistic Data Protection Principles being applied in ever more innovative and challenging scenarios.

The use of privacy policies allows us to frame the business activity and the relationship with the customer, so as to comply with the requirements of the legislation. As such, it remains an invaluable tool in protecting our clients and we would be happy to discuss how we can help you and your business.

Jaan Larner is a business-minded lawyer with an MBA from Oxford University. Jaan is a corporate and commercial lawyer with a particular interest in entrepreneurial activity. He advises clients on their corporate structures as well as their ongoing day-to-day commercial activity.

E: jaan.larner@keystonelaw.co.uk
Smart Cookies – New Rules on the use of cookies came into force on 26 May 2011

The rules on using cookies and similar technologies to store information on a user’s equipment changed on 26 May 2011.

Why has this happened?

The rule change is the result of implementation of an EU Directive. The new rules are contained in Regulation 6 of the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

What do the Regulations cover?

The Regulations cover the use of cookies - small files downloaded onto a device when the user accesses certain websites, allowing the website to recognise the user’s device. They also apply to similar technologies for storing information – including locally stored objects (flash cookies).

What has changed?

Prior to 26 May 2011, if you used cookies to store information, you had to provide clear and comprehensive information to users about your use of cookies and give users the right to opt-out. Many websites complied with this rule by including information about cookies in a privacy policy.

From 26 May 2011, cookies can only be placed on a user’s equipment if the user has given their consent. The requirement to provide clear and comprehensive information remains in place.

Does the new rule apply to all cookies?

Yes – except for one limited exception. Consent does not need to be given where the cookie is “strictly necessary” for a service requested by the user. This is a very narrow exception. For example, it could apply to a cookie used to ensure that where a user clicks “proceed to checkout” when purchasing online, the site remembers the items chosen on a previous page.

This exception is very narrow. The EU Directive on which it is based refers to a service “explicitly requested” by the user and the Information Commissioner, who will enforce these Regulations, will bear this in mind in deciding whether or not the Regulations have been complied with.

Also, the requirement to provide information about a cookie and obtain consent is only required the first time it is set for a particular user. You do not have to do this again for the same person provided that it is the same cookie and is used for the same purpose.
What do you have to do and when?

The government believes there should be a phased approach to implementing these Regulations. However, this does not mean that you should do nothing. The Information Commissioner’s Office has issued initial guidance on the new Regulations which are a starting point rather than a definitive guide. The guidance contains practical steps for you to take now.

- Check what type of cookies you use and how you use them – this may be a comprehensive audit or a simple check of the data files placed on user terminals. Analyse why you use the cookies and decide which are “strictly necessary” and might not require user consent. Use this as an opportunity to clean up your website. The Information Commissioner strongly advises in-house teams to carry out this audit and clean-up exercise in order to demonstrate compliance.

- Assess how intrusive your use of cookies is – the more intrusive your use of cookies, the higher priority you need to give to considering changing how you use them and to obtaining proper meaningful consent from users.

- Decide the best way of obtaining consent for your circumstances – the more intrusive your activities, the more you need to do to get proper meaningful consent. One of the suggestions in the EU Directive and the Regulations is to obtain consent through browser settings. However, the Information Commissioner’s opinion is that, as most browser settings are not currently sophisticated enough to allow you to assume that a user has given specific consent, organisations need to obtain consent another way.

Remember that the Information Commissioner’s Office has made it clear that they are primarily interested in the information gathered through the use of cookies and what organisations do with that information, rather than the cookies themselves.

How do we obtain consent?

- Browser settings – browser level solutions are being worked on at the moment, but the Information Commissioner believes that browser settings are not currently sufficient for users to give consent.

- Pop-ups – this would be acceptable but even the Information Commissioner thinks this might become annoying for users!

- Terms and conditions – there is no reason why consent cannot be included within terms and conditions. However you would need to make users aware of the changes to the terms and conditions and make it explicitly clear that these changes refer to your use of cookies. You would also need the user to positively indicate that they understand and agree to the changes by use of a tick box or something similar. This process must be completely transparent and easily understandable by a user. If you gain consent through users’ ignorance then you will not be compliant with the new rules.

- Settings-led consent – for certain cookies it might be convenient to obtain consent when a user changes the settings for a site. For example, if a user chooses to always access a site in
the English language version, consent could be obtained at the point where the user makes this choice.

- Feature-led consent – similarly, if cookies are stored when a user wants to use a particular feature of a site and the user has to take some action in order to activate that feature, consent can be obtained at that point. If the feature is provided by a third party, you will need to tell users and provide information as to how the third party may use cookies, in order that they can give meaningful consent.

- Functional uses – analytical cookies which collect information about how people access and use your site need user consent, even if they are not so obvious and appear not to be so intrusive. Careful thought will need to be given to the information to be provided and the method for obtaining consent. The Information Commissioner's guidance suggests the use of highlighted text in the footer or header or a web page, or a scrolling piece of text when you want to set a cookie. This could link to the privacy policy on the site which should set out the choices available to the user. Where information about website use is given to third parties, this needs to be made absolutely clear and you should know how the third party uses this information. The Information Commissioner strongly encourages organisations to review their contractual arrangements with third parties concerning the use of such data.

- Third party cookies – this is a difficult area. The Information Commissioner acknowledges that this is the most challenging area for compliance and is working with other bodies, including industry, to try and find the right solutions. However, in the meantime, you will need to work with third parties to ensure that the users are absolutely clear about cookies being set, and that they are able to give meaningful consent.

What next?

More guidance will be issued by the Information Commissioner over time. In particular, guidance on enforcement is expected to be published. Keep an eye on the Information Commissioner’s website for this guidance.

The Information Commissioner will also provide guidance giving examples of methods for obtaining consent and is keen to receive examples from industry. Given the difficulties in obtaining consent, he has stated that he is unlikely to take enforcement action in the first 12 months provided that organisations have taken the steps set out in the guidance. Therefore the current guidance should be followed in order to demonstrate, if any complaint is made, that you have done all you can to comply with the new rules.

Where can I find more information?

The Information Commissioner’s website should be checked regularly for updated guidance

The Initial Guidance from the Information Commissioner

All about Cookies – a website for consumers and marketers which explains the issues surrounding the use of cookies.
Gillian Cordall is an IT, intellectual property and commercial lawyer who advises on commercial arrangements and the protection and exploitation of intellectual property. She has extensive experience in technology, digital media and marketing services contracts and particular expertise in IT and business process outsourcing, software development and licensing and issues affecting online businesses. Gillian is recognised for her work in interactive media, particularly videogames. She is a Trustee of the Society of Computers & Law and Chair of their Media Board.

E: gillian.cordall@keystonelaw.co.uk
T: 020 7152 6550

Disclaimer

We have written these materials to help you, but no article can address all the issues. The benefit of using an experienced lawyer is that they ask the right questions and build the solution around you. Please therefore note that these materials only provide you with general information and should not be regarded as a substitute for taking legal advice.

Would you like to know more?

Keystone is a corporate law firm that has grown rapidly since 2002 when it was set-up to service the SME community. It is a full-service law firm with over 100 partner level solicitors and turnover in excess of £10 million. The firm has a unique structure whereby a central London office supports its solicitors who in turn work from their own satellite offices. Overhead savings are passed onto the firm’s clients who benefit from a very personalised service.

If you would like to know more, or for a competitive quote please call 020 7152 6550 or email enquiries@keystonelaw.co.uk.