Website and email law

Some people think that the Internet is an unregulated free-for-all, but this is simply not the case. The law still applies, although in some areas its interpretation and effects are not entirely clear. And in some cases, such as Internet sales, there are additional laws that give consumers extra rights. The international nature of the Internet, and the ease with which information is copied and transmitted, can lead to additional problems.

This briefing outlines some of the legal issues you need to be aware of. It covers:

- The basic rules covering email and the Internet.
- Contracts, marketing and e-commerce.
- Intellectual property.
- Privacy and data protection.

1 Email basics

The same basic rules which apply to ordinary business letters also apply to emails.

1.1 You need a standard **footer** stating your company name and other details:

- You must include your registered office address, a contact email address, registered number and country of registration.

  You can use the signature feature of most email software to add standard contact details to your emails automatically.

1.2 You may want to include a standard **disclaimer**. A disclaimer might state:

- 'This email is confidential and intended for the use of the intended recipient only. If you have received this email in error, please inform us immediately and then delete it. Unless it specifically states otherwise, this email does not form part of a contract.'

  Simply inserting a disclaimer does not mean that you cannot be held liable for the contents of an email or any breach of privacy that results from it going astray.

1.3 The **content** of an email is covered by the same laws as the contents of a letter.

- Do not send or forward emails that would be illegal, offensive or discriminatory if sent as ordinary documents.
- Check the contractual implications of an email before sending it (see **2.1**).

1.4 Commercial emails are covered by a range of regulations.

- You must clearly show the purpose of the email and who it is coming from.
- You must provide a valid address which recipients can use to opt out of receiving further emails from you.
- You cannot send marketing emails to consumers, sole trader or unincorporated partnerships without their prior consent unless their email address was collected in the course of a previous sale or sale negotiation relating to similar goods or services.
- Any promotional offers contained in your emails must be obvious, clear and easily accessible. Any competitions or games must also be obvious, and the rules both clear and accessible.

1.5 Emails can present high **risks**.

- Emails are easy to distribute widely. A misguided email sent round the office could be forwarded round the world in seconds.
- Emails (and Internet sites) are easily stored and used as evidence.
- If an email is sent (or forwarded) to an international recipient, that country's laws may apply to its content. For example, you might be sued in that country for publishing a libel that may not necessarily be libellous under English law.
- Your business is likely to be held liable for emails sent by employees.

Employees' actions

You are generally responsible for your employees' actions on your email and Internet systems.

A **Contractual obligations** created over the Internet are just as binding as any other.

B **Defamatory** statements are easily circulated to a wide audience.

- Defamatory emails must not be sent or forwarded, even internally.
  Several major companies have already been forced to pay substantial damages to competitors libelled in emails.
- The informal nature of newsgroups and discussion forums means there could be a high risk of employees making defamatory comments.

C Offensive emails or even website access can create a hostile **working environment** and lead to claims for stress or discrimination.

D The Internet can make it easy for employees to commit **illegal acts**, such as stealing other people's intellectual property (see **4**).

- For example, copying photos or text from other sites to use on your own.

In most cases, an aggrieved party will pursue the company rather than the individual employee responsible for the problem. Setting up and enforcing appropriate policies, and providing any training employees need, can substantially reduce the risk of being held liable.

2 Contracts and e-commerce

2.1 An email, or your website, can have **contractual** significance.

- As a seller, you must make it clear what steps a buyer has to take to create a legally binding contract.
- The content of emails sent and received before a contract is concluded can form part of the contractual agreement.
- Digital signatures can be used to authenticate documents.
  Bear in mind that emails are technically digital signatures of sorts and can create legal obligations.
- The information on your website can form part of a contract.
- Make sure it is clear to your customers at what stage a contract will have been formed and the languages it is available in. You must also give customers a chance to check an order for errors (and allow them to correct them) before it is placed.
- On your website you must include your full company name, address (geographic and registered) and email address. The company's registration number and place of registration should also be given. You must also state any professional registration and authorisation scheme (eg the Law Society). If your company has a VAT number, this should be also be stated.

2.2 Take care with your **terms and conditions**.

- Ensure that your terms and conditions are agreed before you accept an order. Send an email to confirm this (provided you have enough stock to fulfil the order).
- Adapt your terms and conditions

specifically for your website. For example, you might want to state that your website is only an invitation to the customer to consider buying from you. Add that the offer will only be confirmed when you email to accept the order.
- Put your terms of trade in a pop-up box that appears when a customer is about to make a purchase over the Internet. Make customers tick a box to confirm they agree to your terms.
  Make sure customers can store a copy of your terms and conditions. For example, put them in a form which can be saved and printed.

2.3 Keep prices — and the rest of your website — **up to date**.

- Make sure you know where prices appear on your site, and check them on a regular basis. Also state whether prices include VAT, tax and delivery costs.
  If your website makes a direct offer, and this is accepted, you may be obliged to fulfil the contract, even if the price is wrong.
- You must clearly indicate taxes and delivery charges, if applicable.
- You must include the buyer's right to cancel the order, known as the cooling-off period. If the customer buys online, they have the right to change their mind and cancel an order for goods within seven working days of receiving the goods.
- Customers also have the right to a cooling-off period for any services or credit agreements they buy online.

2.4 The **place** where contracts and transactions occur can be difficult to determine.

- In some countries, local laws (eg consumer protection laws) will apply even if your terms and conditions state that any contract is governed by English law.
- If you have a presence in another country, and carry out business over the Internet with customers there, transactions may be subject to regulation and taxation in your customers' country.
  If you are using a website to sell or promote your products to UK customers only, make sure you state this clearly.

2.5 Be careful **who** you are selling to.

- Selling to minors may be illegal depending on the country you are selling to and what you are selling.
  You will usually find that contracts with minors are unenforceable.

2.6 You must **confirm receipt** of an electronically placed order without any unnecessary delay.

2.7 If you make **purchases** over the Internet, the same considerations apply.

- Make sure you know who you are dealing with, in which jurisdiction.

Although your website does not in itself constitute an advertisement, you should make sure any adverts carried on it comply with Advertising Standards Authority regulations. The basic rule is that adverts must be 'legal, decent, honest and truthful'.

3 Data protection

Collecting or handling personal data using email or the Internet falls under the Data Protection Act 1998. If you handle personal data in any form, you will have to comply with the Act. You may also have to notify the Information Commissioner annually.

3.1 You must not use an individual's personal data for **direct marketing** purposes if they request you not to do so.

3.2 Set up a clear **privacy policy**, and make it prominently available on your website.

- Before asking users to give information, tell them how their details will be used.
  Will you be using the data for mailings or market research? Will you share their contact information with other organisations?
- It is best practice to have people opt into further use of their personal data for mailings or market research and indeed it is required if you are sharing it with other organisations or are marketing their products.
- Only collect the data you need.
- If your site contains cookies, make visitors aware of this. Cookies can collect contact details and other basic data from users' PCs without their knowledge.

3.3 Make sure you comply with regulations on the **monitoring** of employees' email and Internet use (see **5**).

3.4 Store any data you collect **securely**.

- Access to the data should only be given to employees who need it.

➨ If you are trading abroad, or have any other specific concerns, ask a solicitor. Visit the Law Society's website, www.solicitors-online.com, to find a solicitor with the expertise you need.

4 Intellectual property

4.1 Material on the Internet is **protected** by copyright and other intellectual property laws.

- Put a copyright notice on your website. Actually enforcing your copyright, particularly overseas, can be problematic.
- State any trademarks you are using.
- Do not use images or text that are protected by someone else's copyright or someone else's trademarks without their permission.
- Do not download and use copyright material without permission. For example, you usually have to accept a copyright owner's terms (which may include payment) before downloading software.

4.2 Design right applies to websites.

- If you use a designer to create your own website, ensure that the design right is assigned to you in writing.
  If you fail to do so, you could be forced to pay the designer every time you want to change the site. And you may not be able to have it changed by anyone else.
- Copyright for software you use on your site generally remains with the supplier (and is licensed to you). If you commission bespoke software, get the copyright assigned to you.
  Get a written guarantee from the designer that the site does not breach anyone else's rights.

4.3 Linking to other websites can be a breach of copyright.

- Making other web pages appear to be part of your site, or modifying their appearance, is generally not permitted.

  The safest course is always to ask permission from a website's owner before linking to it.

4.4 Domain names can be contentious. If you have a trademark, and register a related domain name, you should be reasonably safe from potential claims.

- A company that feels you are infringing its trademark can ask the Internet authorities to assign the domain name to them, or take you to court. Large companies are particularly vigorous in pursuing claims (and have the resources to do so).
- Just having a trademark may not be enough to be able to prevent someone else from using a domain name.
  You may have to prove they are acting in bad faith or attempting to piggyback on your success.

5 Monitoring

A monitoring system can help you control inappropriate or illegal use of email and the Internet in your business.

There are legal restrictions on monitoring, although this remains a grey area.

If you are going to monitor emails or Internet use (or phone calls), you must inform employees that you intend to do so. Make it part of your employment contracts and your email and Internet policies.

5.1 In general, you can monitor Internet and email **traffic**.

- You can install software which produces a log of all emails sent and received, together with the addresses (but not the contents).
- You can install software which produces a log of all Internet sites visited and any downloads made.
- You can also install software to prohibit access to specified Internet sites.
- If you do decide to monitor your employees use of email and the Internet, it is essential that you make them aware that you are doing so.

5.2 Under the Regulation of Investigatory Powers Act, you may inspect individual emails without an employee's consent for **specific business purposes**. These include:

- Recording transactions and other important business communications.
- Making sure employees comply both with the law and with your internal policies.
- Preventing abuse of your telecoms system.
- Checking emails when employees are on leave.

5.3 If you wish to monitor communications for **other purposes**, or are not sure whether you have the right to read an email, you must get permission to do so.

- You need permission from both the sender and the receiver.

Published by BHP Information Solutions Ltd, Althorp House, 4-6 Althorp Road, London SW17 7ED
Tel: 020 8672 6844, www.bhpinfosolutions.co.uk