

**THE LEGAL VIEW: SELLING ON THE WEB,  
INCORPORATION OF TERMS, LINKING AGREEMENTS  
AND STAFF COMPUTER USE/EMAIL POLICIES**

**Notes prepared for a talk to the Internet Specialist Group of the BCS on 21 May 2008  
by Jeremy Holt, Head of the Computer Law Group,  
Clark Holt, Commercial Solicitors**

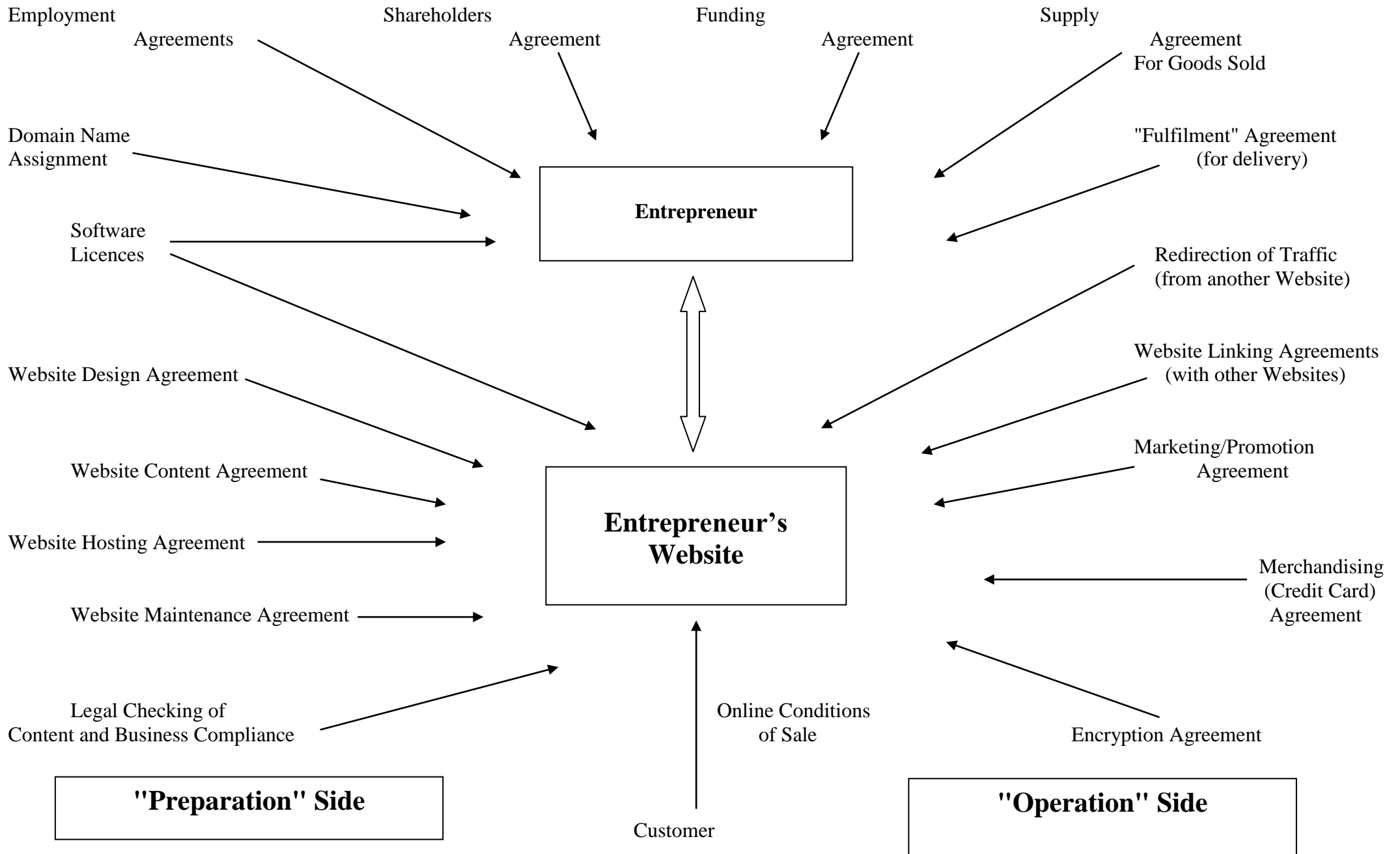
**Clark Holt**  
COMMERCIAL SOLICITORS

**HARDWICK HOUSE, PROSPECT PLACE, SWINDON, SN1 3LJ  
TELEPHONE: 01793 617444 FAX: 01793 617436 DX: 38606 SWINDON (2)  
WWW.CLARKHOLT.COM**

Email: [jeremyh@clarkholt.com](mailto:jeremyh@clarkholt.com)

## **INDEX**

- 1.** Retail Legislation
- 2.** Distance Selling Regulations
- 3.** E-Commerce Regulations
- 4.** Privacy and Electronic Communications Regulations
- 5.** Online Terms
- 6.** Linking Agreements
- 7.** Staff Computer and Email Policies
- 8.** Final Thoughts



## 1. Retail Legislation

*"Who buys has need of a hundred eyes,  
who sells has need of only one"*  
(Proverb)

- Trade Descriptions Act 1968  
This makes it an offence for traders to supply or offer to supply goods or services under a false trade description.
- Consumer Credit Acts 1974 and 2006  
These regulate the full scope of consumer credit activities and include requirements on a range of matters such as documentation, advertising, and the calculation of the cost of credit. They set out rules, not just for credit providers, but also for others involved in the credit industry.
- Sales of Goods Act 1979  
This sets out the law governing contracts for the sale of goods and governs a wide range of matters such as formation of contract, implied terms, remedies for breaches, transfer of ownership and performance of contract.
- Supply of Goods and Services Act 1982  
This covers contracts for services, hire contracts and contracts where goods are transferred other than by a contract of sale. For example, contracts for work and materials including contracts for the installation of goods where there is not a sale of goods contract within the meaning of the Sales of Goods Act.
- The Consumer Protection Act 1987  
This covers product safety and product liability and prohibits the use of misleading price indications among other things.
- Control of Misleading Advertisements Regulations 1988  
These provide protection against misleading advertisements and unacceptable comparative advertisements.
- Unfair Terms in Consumer Contracts Regulations 1999. "Unfair" contract terms are likely to be void in contracts between businesses and consumers unless they have been individually negotiated.

Foreign legislation e.g. Germany's prohibition of "two for one" offers or lifetime guarantees; France's Loi Toubon requires a French language version of any advertisement to or contract with a consumer. At present, member nations of the European Union have widely varying rules for sales promotions and discount schemes. Retailers in Italy must notify the finance minister before launching sales promotions, while Belgian retailers are not allowed to offer discounts of more than 33%. Many EU countries, including Spain and Ireland, forbid below-cost sales.

## 2. **Distance Selling Regulations**

Important rules (the Distance Selling Regulations) apply in relation to the sale of either goods or services by businesses to consumers. The changes related to any sale which is not made face to face but instead is made over the internet, telephone or by catalogue, letter and press advertisement (i.e. what is called "**distance selling**"). Minimum requirements are laid down about information which must be provided to consumers by suppliers. Consumers (which means an individual not carrying on a business) are automatically allowed at least a seven working day cooling-off period during which they can cancel the contract, and all contracts must be completed within 30 days of being made. These rules do **not** apply to business-to-business transactions. There are separate regulations relating to financial services.

### **Minimum Information**

All consumers must be provided with the following information before the contract is made:-

- the name of the supplier and a geographical (rather than an internet) address;
- a description of the goods or services;
- the period that the offer remains open;
- the price (including all taxes);
- **the right to withdraw (see below)**; and
- the arrangements for delivery of any goods.

### **Cooling-Off Period**

Consumers have an automatic seven working day right from the time of the receipt of the goods or the order of the services to withdraw from the sale without giving any reason (commonly known as a "cooling-off period"). **If no details of the cooling-off period have been given by the supplier to the consumer (see above) the cooling-off period is extended by three months.** The right to withdraw can be exercised by the consumer even after the goods have been delivered. If the consumer exercises their right to withdraw no penalty can be charged by the supplier to the consumer (other than the consumer being responsible for the costs of returning the goods to the supplier). Professionals, such as solicitors and accountants, have been slow to appreciate that these cooling-off periods require there to be changes to their standard letters of engagement.

### **Cancellation exceptions**

Consumers do not have to be given cancellation rights for the following goods:

- Clearly personalised goods or goods made specifically to the consumer's specification.
- Goods which, by their nature, cannot be returned or are liable to deteriorate or expire rapidly.
- Computer software or audio/video recordings which have been unsealed by the consumer.

Consumers who exercise their right to cancel must receive a full refund of everything paid under the original contract. This refund must be made as soon as possible but within a maximum of 30 days beginning with the day the notice of cancellation was given.

The only deduction that can be made from the refund is the actual cost of recovering the goods where consumers have breached a contract term requiring them to send the goods back when they cancel.

### **Completion of the Sale**

Unless a longer period is agreed, all contracts must be completed within 30 days of being made. If the supplier is unable to do this because the goods or services are unavailable, the consumer must be told and a refund automatically given by the supplier.

Breach of certain of the rules is a criminal offence by the supplier company (and possibly its directors) and may result in parts of the sale contract being unenforceable. The rules are enforced by the Office of Fair Trading and weights and measures authorities.

The Consumer Protection (Distance Selling) Regulations 2000 can be obtained from the Office of Public Sector Information (OPSI) website at [www.opsi.gov.uk/si/si2000/20002334.htm](http://www.opsi.gov.uk/si/si2000/20002334.htm).

Further amendments to the original DSRs can be found at [www.opsi.gov.uk/si/si2005/20050689.htm](http://www.opsi.gov.uk/si/si2005/20050689.htm).

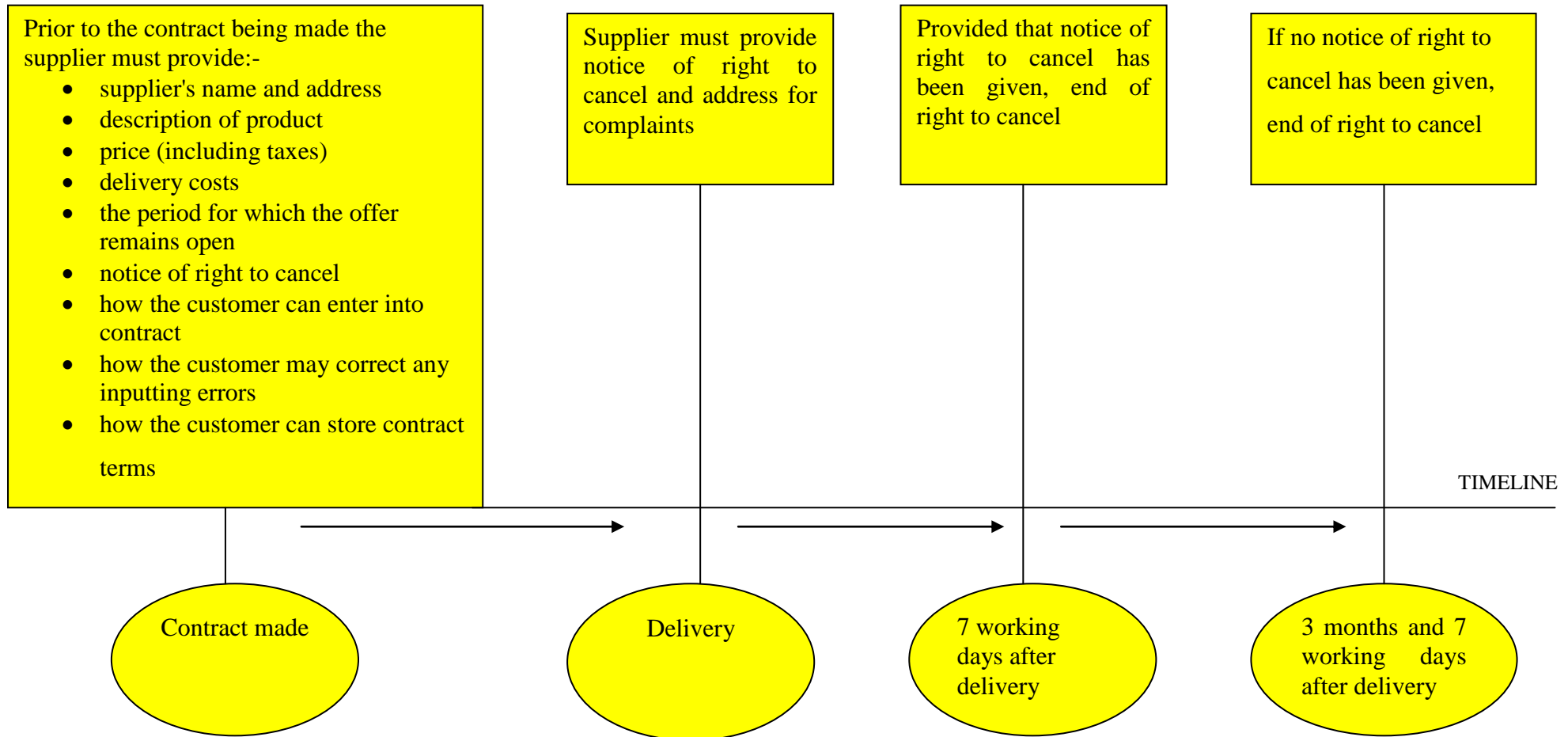
In addition, further guidance on DSRs is available on the DTI website at [www.dti.gov.uk/ccp/topics1/ecommm.htm](http://www.dti.gov.uk/ccp/topics1/ecommm.htm).

In August 2005 the DTI and the OFT published "A guide for businesses on home shopping", which contains a useful summary of some of the practical problems that have arisen.

In December 2005 the OFT published "IT consumer contracts made at a distance". This provides guidance on compliance with the Distance Selling Regulations and the Unfair Terms in Consumer Contracts Regulations specifically in relation to the sale of IT goods or services.

The Distance Selling Regulations have inevitably required suppliers to change both their standard terms and their sale processes (as it is not possible to contract out of most of the Regulations).

## DISTANCE SELLING TO CONSUMERS



### 3. E-Commerce Regulations

Important rules (the Electronic Commerce (EC Directive) Regulations 2002 S.I. No 2013) apply to electronic messages (including text messages and interactive TV). The Regulations were designed to increase confidence in e-commerce. The Regulations apply to all those who:

- provide goods or services to business or consumers on the Internet or by email; or
- advertise on the Internet or by email.

The Regulations do **not** apply to business conducted via fax or voice telephony.

The Regulations required suppliers to provide customers with certain information such as:

- their name, registered office address, registered number, country of registration, email address and VAT number;
- clear indications of prices (including whether they include VAT and delivery costs); and
- details of any trade organisation to which the supplier belongs.

If electronic contracting is carried out the supplier must:

- describe clearly the technical steps required to enter into the contract;
- describe clearly how end users may correct any inputting errors before placing an order;
- describe clearly how end users can access and store the terms of the contract made; and
- acknowledge receipt of an order promptly and electronically and allow the end user must to correct any errors in the order.

#### Marketing by Email

Any form of electronic message designed to promote a supplier must be identified as a commercial communication and specify the organisation on whose behalf it was sent.

Unsolicited commercial communications sent by electronic mail ("spam") must be clearly identifiable as such upon receipt in order to allow the recipient the opportunity to delete it without reading it. One way of doing this is to put "Unsolicited Commercial Communication" in the subject line of the message. In relation to spamming, note also the rights of a data subject under section 11 of the Data Protection Act 1998 to require a data controller to cease using their personal data for direct marketing. This right continues even if the data subject has in the past given their consent to such marketing.

#### 4. **Privacy and Electronic Communications Regulations**

In 2003 substantial changes come into effect in relation to direct marketing by email, automated fax and SMS as a result of the Privacy and Electronic Communications (EC Directive) Regulations 2003. These Regulations replaced the Telecommunications (Data Protection and Privacy) Regulations 1999.

If the rules are breached either OFCOM or a person who has been affected by the breach may refer the matter to the Information Commissioner who can bring enforcement action. It is a criminal offence to fail to comply with any enforcement notice from the Information Commissioner. Personal liability may also attach to company directors or managers for their involvement in such offence. Furthermore, any one who has suffered any damage as a result of a breach can claim compensation from the person in breach.

##### Summary of the New Rules

Under Regulation 22 of the regulations it will be unlawful to send unsolicited emails to individuals UNLESS either

- (a) the sender has obtained the individual's contact details in the course of a sale (or negotiations for a sale) by the sender to the individual AND the direct marketing is about the sender's products AND the individual has been given an opportunity to refuse to receive direct marketing messages when they first gave their details OR
- (b) the individual has notified the sender that they consent to such message being sent. Note that this consent must be a positive act by the individual concerned i.e. an "opt-in" and that consent can not be presumed from a failure to respond.

Whenever the sender sends a message to an individual (a) the individual must be given an easy opportunity at no charge to opt out from future messages and (b) the identity of the sender must not be disguised or concealed.

##### "Cookies"

The regulations also introduced controls on the use of cookies on websites. Cookies are small pieces of computer code used by a website or server that are sent to a user's computer and stored on their hard drive. Their function is to return information to websites so that online user profiles can be created. There are two views of cookies. One is that they are an invasion of privacy. The other is that they are a necessary evil to improve the efficiency of the web. Regulation 6(2) provides that where cookies are used then the individual must be given "clear and comprehensive information" about the purpose of cookies.

## 5. **Online Terms**

Difference between "shrinkwrap" and "clickwrap" licences.

### **Notice of Terms**

- a mere mention
- link to a page that contains the terms (but no requirement to view before contracting)
- terms set out in full and requirement to scroll down them all before contracting
- ideally, a positive act, e.g. have to register or enter a password
- position of repeat customers
- proportionality of terms

Websites can be difficult to navigate. In order to ensure that the prior information is provided in a clear and comprehensible manner, it is sensible to include an 'About Us' page containing your company details and a 'Terms and Conditions' page, both with a direct link from your home page.

There should be a clear and prominent warning that the consumer should read and understand the terms before placing an order. Alternatively, you may ask consumers to tick a box to indicate that they accept the terms and conditions. The terms must be clear, understandable and clearly written, and consumers must have a genuine opportunity to examine and, if necessary, query anything they do not understand.

### **Typical Provisions of a Privacy Policy**

(to be included on a website when information is to be collected)

- collection of information
- use of information collected
- cookies
- links to other sites (disclaimer)
- security of information collected
- opt in/opt out
- correction or updating of information provided
- future changes to the privacy policy

## 6. Linking Agreements

*"Hypertext links are the thread with which the Web is woven"*

(Anonymous)

"Linking" Agreements are agreements made between website owners for the linking (by means of a graphic or hypertext link) of their websites. People surfing the net can go from one site to the other. Such agreements can involve revenue sharing.

Points to consider when drafting such agreements include:

- What type of link will there be? Graphic? Simple hypertext link? Framing link?
- Should there be a ban on links to the other party's competitors?
- What money should be paid?
- What information should each party give to the other about their sites?
- Where will the link be placed?
- How much notice should the party give to the other if they wish to revise their own site?

On a practical level, it is important to check regularly that such links continue to work.

## 7. **Staff Computer and Email Policies**

Employers sometimes wonder whether they have the right to monitor voice calls or e-mail messages and there are a number of myths about this. There is *no* legal distinction between phone calls and e-mail messages for these purposes. Where employers have told employees that their calls will *not* be monitored or given an indication that that is the case then monitoring will be in breach of both the terms of employment and of the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699 ("the Regulations") came into force in 2000. The Regulations state that it is lawful for an employer to monitor and record certain types of communications in restricted circumstances without the consent of the sender or recipient. Without the Regulations the employer would be in breach of the Regulation of Investigatory Powers Act 2000. Under the Regulations an employer who wants to intercept communications must make all reasonable efforts to inform every person who may use the system that interception may take place. This is easy with employees as notification of monitoring can be given. It is more difficult with third parties. One possibility is to include an automatic warning about monitoring at the end of all external emails.

Employers should remember that even if interception of messages is carried out by them in a legitimate manner, any use by them of the information gathered must be proportionate and in accordance with the data protection legislation (e.g. it should not be passed on to third parties without good cause or the consent of the employee concerned). The data protection legislation prohibits the abuse of data about living individuals e.g. by such data being used for purposes for which the individual has not consented. The Information Commissioner (who deals with data protection) has published a code on monitoring at work.

Although this code does not have the force of law it can be used in any enforcement action by the Information Commissioner and may be referred to in employment tribunal proceedings. The code emphasises that monitoring of messages should only take place when there is a real business need and the methods used should not be unduly intrusive into an employee's privacy. Employees have a reasonable expectation that they can keep their personal lives private which means that they are entitled to some privacy at work. It is recommended that employers should wherever possible avoid opening emails, especially ones that clearly show that they are private or personal. Employees should be aware that monitoring is taking place and told the reasons for it and the means used. Covert monitoring will only be legitimate in the most exceptional of circumstances such as the detection of crime or equivalent wrongdoing. It is good practice for the monitoring to be carried out by someone other than the employee's line manager e.g. security or human resources. In this way, such personal information that is picked up about employees can be sifted so that only the most relevant ever becomes known by those who work with the employee.

You need to get the security policy across to everyone using the employer's computers (who, of course, are not necessarily all employees). The staff handbook and employment terms are a means to that end backed by emphasis on induction.

I have read of one employer who gives new employees a copy of the Computer Misuse Act 1990 when they start (they cost £3.40 each from TSO, formerly HMSO, telephone 0870 600 5522). They are also available free online from: [www.opsi.gov.uk](http://www.opsi.gov.uk) (the ISBN of the Computer Misuse Act 1990 is 010 541 8900).

The point can be backed up by reminders on computer screens and regular training. The same rules should also be applied to any in-coming freelance contractors (often overlooked). Internal audits should check that security policies are being followed and the side should not be let down by senior management (as it frequently is). The aim should be that no user of the firm's computers could reasonably argue that they were not aware of the rules of use.

## **SPECIMEN COMPUTER AND EMAIL USE POLICY**

We do not wish to restrict in any way your use of our computer system – indeed we encourage it. However we regard the integrity of our computer system as key to the success of our business. To avoid misunderstanding and confusion all employees must abide by the following policies. Breaches of this policy will be taken seriously and could amount to gross misconduct. You should direct any queries about this policy to the HR Department.

### **1. Licensed Software**

Only properly licensed software may be loaded onto our system. You are not allowed to use within the company any material that you either know, or suspect to be, in breach of copyright. In addition, you are not allowed to pass such material on to anyone else. It is important to bear in mind that breach of copyright for business purposes can be a criminal offence both by the company *and* by the individual concerned. No software may be loaded onto our system without first obtaining the express permission of the IT Department. Software includes business applications, shareware, entertainment software, games, screensavers, and demonstration software. If you are unsure whether a piece of software requires a licence, please contact the IT Department. The copying of software media and manuals is also prohibited.

### **2. Networks**

You are not allowed to make any change to the connection or configuration of your PC. None of our PC's may be connected to a customer's network without both permission from the IT Department and written permission from the customer concerned. In addition, none of our PC's may be connected to a public network, e.g. internet, without permission from the IT Department.

### **3. Disks**

You must not use disks from unknown sources or from home computers. All data disks must be virus checked before they may be used on our computer system.

### **4. Viruses**

Generally, more damage to files is caused by inappropriate corrective action than by viruses themselves. If a virus is suspected you should do nothing more until instructed. The matter must be reported immediately to the IT Department. The most likely way that our computer system will be infected by a virus is by an external message. Any outside material must be properly virus checked before being loaded on to our computer system. Many viruses are now spread by email messages and use the address book of the recipient to pass it on to other people. Some of these viruses are activated when an attachment to the message is opened. Creators of these viruses frequently encourage the user to open the attachment simply by using a header such as "You must read this!" You should not open any attachment of this type and must generally be suspicious of any message that is received from an unknown source. In other words, only open mail when you know it is from a reliable source. If you receive email warnings about viruses please ignore the instructions they contain.

In the majority of cases they are hoaxes and the instructions, if followed, will damage our computer system.

5. **Customer Procedures**

If you use a customer's computer system you must observe the customer's rules relating to their computers. In the absence of any such rules our rules should be followed.

6. **Access**

You are only allowed access to those parts of our computer system which you need in order to carry out your normal duties.

7. **Inappropriate Material**

You must not view or download or pass on any pornographic material on our computer system or place obscene or offensive screensavers on your PC. In line with the normal rules that apply to you as an employee, you are not allowed to send racist, sexist, blasphemous, defamatory, obscene, indecent or abusive messages on our computer system, either internally or externally. Do be careful and think carefully before sending any questionable messages that could reflect badly on us as a company.

8. **Use of the internet at work**

The primary reason for our providing you with access to the internet and/or email is to assist you in your work for us. You are allowed to send personal emails in a similar way to the way that minor incidental personal telephone use is allowed. However, personal emails should be kept to a minimum and the company's footer **MUST NOT** be shown on a personal email. Such activity should not be excessive and must not affect your ability to work properly for us during normal working hours. You are not allowed to go onto the internet for your own purposes during normal working hours. You are allowed to do so outside normal working hours (and during your lunch hour).

You are not allowed to send unsolicited emails or email messages to multiple recipients or use email for personal gain. You are also not allowed to use the company's internet access and email system to sign up for online shopping or internet membership schemes or chatrooms.

For the avoidance of doubt, you are not allowed to disclose any confidential information or trade secrets, nor to defame, harass or bully any third party using any blog or similar web forum.

9. **Orders**

You must not order anything on our behalf by email without proper authorisation. You should always bear in mind that an email from the company has the same legal effect as a letter from the company on the company's notepaper. This underlines the importance of being careful with what you say in an email in case it is misunderstood.

All company emails must contain our standard footer which will be notified to you from time to time. As stated above, personal emails must not contain the company's standard footer.

10. **Confidentiality**

Before sending any confidential information by email consider carefully whether appropriate steps have been taken to maintain such confidentiality. Email is not inherently a more secure medium of communication than traditional means, and can be easily copied, forwarded and stored.

11. **Security**

Do not give internal passwords to anyone outside the company. In addition, you must not give any customer-related security information to anyone other than the customer unless specifically authorised in writing by the customer in advance.

12. **Records**

Keep proper records of our dealings with outsiders. It is always possible that what appears to be a relatively trivial point could be of immense significance later. It is not possible to foresee what will subsequently need to be checked so keep a complete record of all transactions.

13. **Data Protection**

If you have access to data about individuals you must bear in mind at all times the provisions of the Data Protection Act 1998. Guidance on these may be obtained from the Personnel Department.

14. **Passwords**

Use passwords at all times and change them at the intervals notified to you. Do not select obvious passwords. All passwords must be kept confidential.

15. **Backups**

Regular back-ups must be carried out in accordance with the rules laid down from time to time. Critical information should not be stored on the hard disk of your workstation in case it is lost.

16. **Misuse**

Misuse of computers is a serious disciplinary offence. The following are examples of misuse:

- (a) fraud and theft
- (b) system sabotage
- (c) introduction of viruses and time bombs

- (d) using unauthorised software
- (e) obtaining unauthorised access
- (f) using the system for unauthorised private work or game playing
- (g) breaches of the Data Protection Act 1998
- (h) sending abusive, rude or defamatory messages via email
- (i) hacking or
- (j) breach of the company's security procedures or this policy.

This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct, punishable by dismissal without notice. Misuse amounting to criminal conduct may be reported by us to the Police.

17. **Breaches**

All breaches of computer security must be referred to the IT Department. If you suspect that a fellow employee (of whatever seniority) is abusing the computer system you may speak in confidence to the HR Department. You are responsible for any actions that are taken against us by a third party arising from restricted and/or offensive material being displayed on or sent by you through our computer system.

18. **Monitoring**

**The company reserves the right to intercept and monitor your communications, including email, internet and telephone calls.** This right to monitor may be exercised, for example, for the purpose of deciding whether communications are relevant to the business, for the purpose of preventing or detecting crime or to ensure the effective operation of the system.

In addition, the company reserves the right to monitor communications in order to determine the existence of facts, to detect unauthorised use of the system and to decide the standards which ought to be achieved by employees using the system.

19. **Improvements**

We welcome suggestions from you for the improvement of this policy. These should be directed to the Personnel Department.

## 8. Final Thoughts

*"It is always a silly thing to give advice,  
but to give good advice is absolutely fatal"*

(Oscar Wilde)

- Do not be disheartened that you do not know very much. Very few people have had more than a few years' experience of this in this country. Look at the positive side of the massive opportunities that it offers.
- Grab every opportunity to find out more about what is happening either by talking to those involved or by reading publications such as Computer Weekly, the Economist or the Financial Times. Read some of the many books on the subject. Communicate your enthusiasm for the subject; people like enthusiasm – there is not enough of it about.
- The wind blows from the west. It is sometimes said (not always accurately) that half of the users of the internet are in the United States. Follow what is going on there.
- Think internationally. So far as the internet is concerned national borders are the equivalent of our county boundaries. *"Think Global, Act Local"*.
- Join the Society for Computers and Law – 0117 923 7393; ([www.scl.org](http://www.scl.org)).
- Subscribe to the "Internet Newsletter for Lawyers" published by Delia Venables 01273 472424 ([www.venables.co.uk](http://www.venables.co.uk)).
- Try to anticipate the future. From your reading and your experience in this area, what do you think will happen next? What advice will therefore be required?