Software use and your legal liabilities

Computer software is a central part of many businesses' operations. But its increased importance brings new risks. Fraud, viruses, legal challenges and simple mistakes can all have catastrophic effects on your profitability.

An effective software policy is essential, even for small businesses. This briefing outlines:

- Why you need a policy.
- How to draw up a policy to minimise your legal and commercial risks.
- How to purchase and control software.
- How to implement your policy.

1 Software policy cuts risks

Setting up a software policy may not seem like a pressing concern. But without one, your business will be exposed to a range of risks — some of which could be highly damaging.

1.1 A good policy will reduce the risk of **viruses** and other security problems.

- Viruses could wipe out some or all of your data — and could even cause your whole network to crash.
- Games and similar software downloaded from the Internet are particularly likely to carry viruses.
- Illegal software may contain bugs which could be equally damaging.

See **Security and the Internet**.

1.2 It will protect you against possible **legal problems** (see **2**).

- Penalties for software piracy include an unlimited fine, or even a prison sentence.

1.3 It will help ensure you receive the **technical support** you need.

- If you have illegal or poor-quality software, you will not have access to support services provided by the software publisher.
- Neither will you be notified of known problems, or be entitled to upgrades.

1.4 It will minimise **inefficiency** and wasted time (see box, page 2).

2 Legal basics

2.1 When you 'buy' software, you usually purchase a **licence**.

This sets out exactly how you can use the software.

- Almost all standard software packages are sold with a licence.
  If you commission bespoke software, you can have the copyright assigned to you.
- The licence will specify how many copies you can make (and use).
  Unless the licence states otherwise, you may only use one copy of the software on one computer, although many licences allow you to retain up to two copies for back-up purposes.
- Some licences place restrictions on who may use the software, and for what purposes.
  Some software is provided free, or at a reduced price, for academic or personal use. Commercial use of such software is prohibited.

2.2 Breaching the licence is **software piracy**.

Typical breaches include:

- Making or selling illegal copies.
- Using illegal copies of software, even unknowingly.
- Using legally acquired software on more computers than the licence allows.
- Allowing employees, or other contacts, to make unlicensed copies of software.
- Allowing a consultant to install software on your system when you do not have a licence for it.

2.3 Software piracy is a **criminal offence**.

- You risk up to two years in jail, or an unlimited fine.

2.4 Software publishers may **sue you** for piracy.

- You can be sued for any improper use of their intellectual property (see **2.2**).
- Damages can run to tens of thousands of pounds.
  They are normally linked to the amount of money lost, which depends on the number of illegal copies and the length of time they have been in use.
- You also face the possibility of the expense and disruption of legal action, regardless of whether you have to go to court.

2.5 It can be easier than you think to be **found out**.

- The software publishers' trade association, the Business Software Alliance (BSA), offers a reward of up to £10,000 for information on the illegal use of software.
- Disgruntled employees or ex-employees may inform on you.
- Any consultant or company you use to support your IT system is likely to discover any illegal software.

2.6 Your **reputation** could suffer if it is made public that your business has been using illegal software.

Increase your efficiency

A good software policy will not just protect you against the risks inherent in using illegal software — it can also help you work more efficiently. It will:

A Make sure employees have exactly the software they **need**.

- Providing expensive software to employees who do not need it is wasteful.
- Failing to provide software which will improve efficiency can be just as expensive.

B Improve your software **planning** and control.

- It makes it easier to identify and control any software upgrades, and any related training requirements.
- You will gain a better understanding of total IT costs and usage.

C Reduce **time-wasting** and errors.

- You can ensure that all employees use compatible systems.
- Finding documentation when necessary is easier if it is sensibly filed.

3 Developing a policy

Your software policy will need to cover a number of different areas.

To maximise its effectiveness, give one employee overall responsibility for developing and implementing it. He or she should:

3.1 Identify the software you already have, and any you may need.

- This information should be entered on a register of software assets (see **5**).

3.2 Allocate software to individual employees, according to their particular needs (see box).

3.3 Arrange appropriate **training** in the use of software.

- There is no point buying expensive software and then failing to train employees in its use.

3.4 **Authorise** all software purchases and installations (see **4**).

- Central purchasing may reduce costs, and will make it easier to track software.

3.5 **Upgrade** software when necessary.

3.6 Check the software policy is being applied and **enforced** properly (see **6**).

- The same individual may also take responsibility for enforcing other aspects of your IT policy.

4 Acquiring software

Being careful about how you buy and install software is essential if you want to be sure it is legitimate.

4.1 Only buy software from **reputable sources**.

- Typically, this will be a reputable dealer, or a partner outlet recognised by the software publisher.
- If in doubt, make further checks (see **4.2**), or buy the software elsewhere.
- Be particularly wary of software sold through e-auction houses, as much of it is illegal.
  You also risk paying for software you will never actually receive.

4.2 Carry out some basic **checks** to make sure the software is legitimate.

- Software packages should typically contain a licence document with a serial number, a registration card and a manual.
  If you are buying multiple copies of software for use on a number of computers, you may only receive one licence document.
  Pre-installed software supplied with computers may only have an electronic manual.
- Check the packaging.
  Poor quality labels, photocopied manuals and the like are often signs of pirated material.
- If you are still unsure, check the licence number with the software publisher, preferably before you buy.

4.3 Make sure the individual responsible for software policy approves **all software installations**.

As well as new software packages you have purchased, these approvals should include:

- Free software, or software which can be downloaded from the Internet.
- Software upgrades.
- Installation on additional computers of software you already use.
- Employees' personal software for their own use.
  It is probably best to ban employees from using their own software on your system.

5 The software register

A software register is the simplest way of keeping tabs on the software you are using, helping you to control purchases and upgrades and pre-empt potential licence problems.

5.1 Create an **inventory** of all the software you use.

- Record the product name, version number and serial number for every software package on every computer.
- Note down the same details for software you have not yet installed.
- If you own licences which allow you to use multiple copies of a piece of software, record how many copies are installed, and on which computers.
- Include details of any software pre-installed on computers you have bought.

Keep all the information in a secure software register.

5.2 Identify and correct any **problems**.

- Uninstall copies of unlicensed software, or purchase the necessary licences.
- If you are using too many copies of licensed software, you may need to buy more licences.
- If any computers have unnecessary or unauthorised software installed, uninstall it. This will release computer disk space and can improve your system's performance.
- Consider upgrading any outdated copies of software so all users have the same version.

5.3 Routinely **update** your software register.

- Amend the register whenever you purchase or install new software.

- Conduct an audit of the software on each computer at least once a year.
- Undertake intermittent spot-checks if you suspect any problems.

5.4 Store original software and documentation securely.

This should include original software CDs or floppy disks, and any manuals, licence documents and invoice details.

- If you cannot find all the relevant information, you may want to contact the software publisher to check your software is legitimate.
- Protect original software against unauthorised copying.
- File manuals and documentation properly so you can find them easily.

6 Making it work

6.1 Communicate the policy to all employees.

- Tell them you do not allow the use of illegal, pirated software.
- Consider referring to the policy in your statement of employment terms (see Employment contracts).
  Alternatively, ask employees to sign a statement saying they understand and accept the policy.
- Regularly remind employees of the policy, particularly when breaches are suspected.
- Encourage employees to tell you if they think they may have dubious software, or if they have any other concerns.

6.2 Rigorously **enforce** the policy.

- Make following your software policy a disciplinary requirement.
- The more effort you put into enforcing your policy and making sure employees know the use of illegal software is not acceptable, the less vulnerable you will be.
  Showing that you made all reasonable efforts to prevent unauthorised use of software helps protect you against legal claims if an employee breaches the policy.

6.3 Make your software policy part of a wider **IT policy** designed to safeguard the security of your systems and data and protect you against a range of legal risks.

This should:

- State what you consider to be acceptable and unacceptable use of your IT system.
- Set out who is responsible for administering and repairing systems and enforcing your policy.
- Regulate how the Internet and email are used.
- Protect your intellectual property rights. Employees can use the Internet and email to copy and pass on your intellectual property or other confidential material, perhaps unwittingly.
  Implementing an effective policy and a good document management system is essential.

See Website and email law, An Internet policy for your employees, An email policy for your employees, and IT disaster prevention.

7 Further information

7.1 The **Business Software Alliance** offers free tools and resources on its website at www.bsa.org/uk.

- These include a guide to managing your software assets, auditing tools, a list of asset resource management services and a software audit return form.
  You can also find hints and tips on what to look for and what to avoid when buying software.

7.2 Individual software publishers have their own systems for checking whether software is pirated.

- For example, Microsoft runs a Product Identification Service designed to support customers wanting to make sure they are acting within the law.
  Visit www.microsoft.com/uk/piracy/genuine/default.mspx.

Further help

There are other Directors' Briefing titles that can help you. These briefings are referred to in the text by name, such as Website and email law.

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