Remote working

Laptop computers, mobile phones and other technologies mean that some businesses do not need a physical 'place of work' for their employees.

Even if you are not ready to do away with company premises altogether, remote working can still help your business become more efficient.

This briefing covers:

- What you can do with mobile working.
- Understanding the options available.
- Choosing the right set up for your business.

1 Remote working explained

1.1 Remote working enables your employees to **perform their duties** without having to be present on your premises.

Remote working can include:

- Working from home.
- Working while out and about — for instance, on the train or in a cafe.
- Working at client sites — for instance, at a meeting or training day.

1.2 Implemented correctly, remote working can bring a number of **benefits** to your business.

- Extra efficiency.
  Your staff can work at times when it was previously impractical, such as on the train.
- Additional flexibility.
  To some extent, you can allow your employees to work when and where they want.

- Lower overheads.
  With fewer staff onsite at any one time, you can manage with smaller premises.

1.3 There can be **management issues**.

- It is harder to manage teams of people working remotely.
- You need to trust your staff to work unsupervised.

2 What you can do

2.1 Remote working usually utilises technology to make available **resources** which were previously only available in a single location.

Examples of what you can do with remote working include:

Directors' Briefing

a book in four pages

More than 160 briefings are now available.

If you need further information or help, ask the distributor of this briefing about the services available to you.

- Send and receive email from any location, with a laptop or mobile phone.
- Connect to the office network using a laptop and broadband connection.
  This allows you to securely access everything you can normally access in the office, like the latest stock information.
- Conduct remote meetings using a teleconferencing service or online meeting space.
- Divert phone calls to your current location. Even though you may be at home, the caller still rings your office number.
- With a telephone, laptop and broadband connection, some employees can do everything at home which they usually do in the office.

3 The hardware

You do not need specialised hardware to implement remote working.

Exactly what you do need will depend on what level of remote working you wish to adopt.

3.1 Modern **laptop computers** can do virtually everything a full-size desktop machine can do, with the bonus of portability.

- By issuing laptop PCs as standard, remote working becomes much easier to implement.
- You will pay a slight premium for a laptop with a specification equivalent to a desktop computer.
  However, it is often worth it for the additional flexibility.
- Demanding programs like graphic design software may need a particularly powerful (and therefore expensive) laptop.
  Mid-range machines can run typical office software with ease.
- If a laptop is frequently used 'on the road', check the size, weight and battery life carefully.

3.2 A **network server** provides a central store for documents.

- Your staff can then log in to the server and access files across the Internet.
- You will probably need to provide a VPN to allow secure access to business resources. This can consist of hardware and/or software. See 4.4.
- See Network servers.

3.3 **Mobile telephones** can keep staff in touch wherever they are.

- Basic handsets allow you to make calls and send and receive text messages.
- More powerful 'smartphones' allow you to send and receive email and run cut down versions of standard software packages. They are a very effective way to keep up with emails on the road.
- When purchasing mobile phones, look at the overall cost of the tariff carefully and be wary of long contracts.
- Personal use of company mobiles can be a problem.
  Make sure you have a policy governing this. See **6**.

3.4 **Broadband** enables employees to use the Internet, access company resources and send and receive email from home.

- If you plan to allow employees to work from home, you may need to provide them with an Internet connection.
- The most common type of broadband uses a conventional telephone line.
  Also called ADSL, it is adequate for most tasks and cost-effective.
- Broadband typically costs from £10 a month.
  See Specifying and purchasing IT.
- If your staff will be working from home frequently, look for a broadband provider which guarantees a certain level of service and does not impose data transfer limits.
- Mobile broadband connections are also available.
  These provide broadband-like speeds through a small device connected to a laptop.
- Mobile broadband coverage is patchy, so check carefully before purchasing.

3.5 **Forwarding telephones** allow staff to receive calls wherever they are.

- When away from the office, your employees can forward calls to their mobile telephone or another landline.
- Many telephone systems offer forwarding as standard.
- Alternatively, you could consider a Voice over Internet protocol (VoIP) system that routes calls over the Internet.
  See Telecoms for competitive advantage.

4 The applications and software

4.1 You can provide basic remote access to emails with a **webmail** system.

- Webmail allows you to access your email through a standard web browser, like Internet Explorer.
- Typically, you type in a user name and password to access an email account.
- You can then view messages and send them as normal.
- Free webmail services include Hotmail, Yahoo! Mail and Google Mail.
- Web hosting companies can also supply webmail access to email addresses.
  See **Setting up a basic IT system** and **Email, calendars and instant messaging**.

4.2 Other tools can help your employees work

Remote working on a budget

You do not need to spend big to see benefits from remote working.

A   Most **mobile phones** purchased in the last three years have email built in.

- You should be able to set it up by inputting your server details, username and password.
- This will allow you to send and receive email on the move.
- Check whether your email addresses can be accessed using IMAP.
  This holds all your messages on a central server and means you can view them wherever you are.
- Many handsets also have basic Internet browsers to access websites.

B   **Laptops** are a viable alternative to desktop PCs, and not much more expensive.

- As you replace old PCs, consider moving to laptops as standard.
- This will enable you to test out remote working and introduce it gradually.
- A new breed of cut-down laptops has appeared.
  These small, light 'netbooks' cost around £200 and are ideal for document editing and using the Internet.

C   Many remote working tools are **free or very cheap**.

- Free wireless Internet access is available in many cafes and public spaces.
- Online backup services allow you to upload files to share with co-workers.
- Instant messaging software is usually free, and a good way to keep in touch with colleagues.

---

together remotely.

- Teleconferencing services allow you to hold meetings with several people in a telephone conference call.
- These services include Powwownow (www. powwownow.com) and GoToMeeting (www.gotomeeting.co.uk).
- Online collaboration services let you work with a team on projects.
  Examples include Basecamp (www. basecamphq.com) and Huddle (www. huddle.net).

4.3 An **extranet** allows you access to files and folders remotely.

- An extranet is a version of your company intranet which staff can log in to over the Internet.
- Once logged in, they can view documents and download files.
- An extranet is good for providing limited access to important resources.
  For more complete access, consider a virtual private network (see 4.4).
- See **Intranets**.

4.4 A **virtual private network** (VPN) can provide complete access to the company network.

- A VPN creates a secure connection between a remote computer and your office network across the Internet.
- It is the best way of enabling employees to access company resources, and makes remote working much more practical.
- It is very important your VPN is secure. Because of this, setting up and maintaining a VPN is a job for an expert.
- You may need to purchase specialist software and hardware to create a VPN. Your IT supplier or a consultant should be able to advise.

5   Connections

Security risks increase with remote working. The dangers are manageable, but it is important to take security precautions.

5.1 Remote working usually involves transferring **important data** across the Internet.

- Hackers could intercept this information or try to break into your computer.
- Make sure all your company computers run up-to-date security software, including a firewall.

- Only connect to your company extranet, VPN or email using computers and connections which you trust.
- Use encryption to scramble sensitive data. This makes the data unreadable, even if intercepted. Microsoft Windows includes encryption, or you can download encryption software online.

5.2 It is possible to break into remote access systems by **guessing** usernames and passwords.

- Make sure all your staff have strong passwords.
  For example, you can often set up systems so they require passwords to be a certain length and contain both numbers and letters.
- Consider using other ways to log in to your systems.
  For instance, many VPNs require something you have (a smartcard) and something you know (a password).

5.3 Portable devices like laptops and mobile phones are easily **misplaced or stolen**.

This can be disastrous if they contain confidential information.

- Try to store data on a central server rather than on individual laptops.
  See **Network servers**.
- Always back up data.
  Often the value of data on a laptop exceeds the value of the laptop itself.
- Some laptops have encrypted hard drives, which makes it hard for unauthorised users to access the data.
- Make sure company policies include guidance on good practice with equipment.
  For example, employees should not carry laptops in readily-identifiable laptop bags, or leave them visible in cars.
- Ensure you have adequate insurance cover for all devices in your business.
  Try to keep spares in stock for immediate replacement.

See **IT security**.

6 Management issues

6.1 Managing staff who are not in the office can be challenging.

- Ensure all staff are easily contactable when they are working remotely.
- You may wish to ensure that all staff spend some time in the office.
  You could run team meetings to get everyone together regularly.
- You can use monitoring software to track your employees' work.
  However, this can lead to resentment and distrust.
- Fairness is important.
  Your company policies should lay out exactly when remote working is acceptable, and what everyone's obligations are.

6.2 Minimise the **information security risks**.

- Ensure that employees are aware of basic good practice.
- Stress the importance of complying with security procedures such as using passwords properly and regularly backing up files.
  If possible, avoid storing confidential information on portables.
- See **IT security**.

6.3 Make sure that portable devices do not fall outside your **regular IT management systems**.

- If office portables are shared, set up a system recording who has been issued with them.
- It can be tempting for employees to use their own portable devices if it makes their job easier.
  Be clear that this is unacceptable, and have it written into your IT security policy.

6.4 Be aware of potential **health and safety risks**.

- Prolonged use of laptops carries a greater risk of problems such as eyestrain or RSI.
- If an employee will be using a laptop as an office computer, provide an external keyboard, monitor and mouse.