

Guide from [insert your firm's name here]

Tel: [insert telephone number here] Email: [insert email address here] [Insert web address here]

[Insert a line about your business here]

Maintaining your IT system

Regular IT maintenance helps protect your data and reduce the risk of serious IT problems. You also need to be able to deal with any hardware and software issues that do arise.

There are simple steps you can take yourself to minimise risks and tackle problems. You should also make sure you have the right suppliers and support services.

1. Suppliers and warranties

Start planning your maintenance strategy before buying your equipment. Cheap equipment can be a false economy, especially if it is required to support key applications. Look for business grade equipment when purchasing desktop PCs and laptops.

If you lack in-house technical expertise, aim to arrange on-site maintenance

- On-site maintenance means the supplier will come to you to carry out maintenance tasks.
- Choose a supplier that offers at least one year's on-site maintenance.
- If this is not included, ask how much on-site cover would cost. If the cost is below 15% of the purchase price, it is probably a good investment.

A return-to-base maintenance deal may be sufficient if you have some expertise

- For example, if you have some technical expertise but have never fitted new parts.
- Make sure you have enough computers to keep your business working if you have to send one off for repair.
- Check who pays the shipping costs if you have to send back a large piece of equipment.
- Critical hardware like network servers should always have on-site cover.

Paying for extra cover may not be worthwhile if employees have proven experience

- Do not overrate your employees' capabilities.
- Check that opening PCs to add or replace components will not invalidate the warranty.
- Once the standard warranty has expired, or if software or network problems occur, a good relationship with a local IT supplier may be worth more than extended hardware cover from the manufacturer.

Pick a supplier that will give you the original licences for pre-installed software

- Most software can now be downloaded and reinstalled over the internet and updated automatically. This makes maintenance simpler.

Check equipment carefully on delivery

- Do not install anything until missing items have been supplied.
- If you have room, keep the packaging - at least for a short while. It makes returning equipment easier.

Equipment is most likely to demonstrate a fault when it is first powered up

- A common cause of computer failure is components coming adrift during transit.
- If a new computer will not start, check all cables and connections and try again.
- If the problem persists, contact the supplier for a replacement.

2. The office environment

The environment can have a dramatic effect on the performance and reliability of IT systems.

Do not place equipment near radiators, water or sources of dust

- Keep air intake vents clear from dust. Computers get very hot while in use (temperatures of central processors can reach 80-100°C) so they need good airflow to avoid overheating.
- Use a can of compressed air to blow dust out from the vents.

All cables should be as short as possible

- Use cable ties for a tidy and safe office.
- Where possible, always favour Wi-Fi connections over Ethernet in order to reduce how much cabling is required.
- Loose connectors are a common cause of problems. Ensure screws are firm, but not over tight.

Modern computers are generally reliable

- Computers can be left on 24 hours a day but switching computers off each evening is more energy efficient. Use hibernation modes to make powering them up faster.
- Unexpected power failures can cause damage and data loss. Connect key hardware to an uninterruptible power supply (UPS). This will provide backup power so you can shut the hardware down properly.

3. Looking after your data

Looking after your data should be one of your highest priorities. A loss of key data (eg your customer database) can have catastrophic consequences.

Store data both onsite and on the cloud

- Data stored on the cloud can be accessed from any computer, but it's still advisable to keep local copies in case of an internet failure.
- You should regularly back up your data both onsite and to the cloud.

Make sure everyone in your business saves files in standard locations

- It can be hard to locate files without a structured system of folders.

- You can give each employee their own area on your server and cloud storage platform (which are usually linked).

Manage your hard disks

- Hard disks may slow down if the data stored on them is too fragmented. You should run a defragmentation utility every six months. This rearranges the data on the hard disk more efficiently.
- If you run short of hard disk space, start by archiving and deleting files to which you no longer need immediate access. Files relating to complete projects can be archived onto a separate drive, and then removed from your main hard disk.

Viruses and cyber security

Viruses, spyware and hackers are all serious threats to your company's data. Always take security precautions, and seek expert advice if you are in any doubt as to what you need.

Install security software on all your devices

- Respected security software packages come from Symantec, McAfee and Sophos amongst others.
- A security package should include anti-virus and anti-spyware software, plus a firewall and email protection.
- Many packages include additional tools to help you identify suspect websites, emails and other threats.

Minimise the risk of viruses entering your system

- Always buy software from reputable distributors.
- Do not allow employees to download unauthorised software or files.
- Ban employees from opening attachments to unexpected emails, no matter what their apparent source.
- Make sure every external file is checked for potential viruses.
- Do not allow employees to use file-sharing software.

Set up firewalls

- Firewalls help prevent outside users gaining access to (hacking into) your system.
- Every device should have a firewall installed (these often come as standard with the operating system).
- You should also use a hardware firewall. This sits in between your company network and the internet. Most internet routers have a hardware firewall built in.

4. Identifying problems

PC problems are often hard to pinpoint. It may be difficult to know whether it is a hardware, software or connection problem.

Many faults occur intermittently or seemingly at random

- These are often the most difficult to cure.
- If the fault can be replicated, identify precisely what triggers the problem.

Hardware faults usually affect all applications

- If a fault only appears in one application, it is probably a software problem.

There are diagnostic tools you can use to test hardware

- Look for software from security firms like Symantec or McAfee.

Unusual noises coming from a computer may indicate a hardware fault

- Whining, knocking noises, or a recurrent 'ching ching' sound, may mean a hard disk is about to fail. If you have not already backed up your data, do so immediately.
- Any unusual noises should be dealt with promptly. They can give you valuable early warning of serious problems. If you have no in-house expertise, contact your supplier.

A failing monitor sometimes produces sudden changes in the picture on the screen

- It may shrink down and then go back to its original size, or wobble and flicker - or you may hear strange noises.
- Do not assume a monitor has failed just because you cannot see an image on the screen. Check to see if the brightness or contrast has been turned down and that all cables are connected.

The output from a laser or inkjet printer may be streaky, patchy or missing colours

- The problem may be an empty cartridge. Try new cartridges.
- It is usually cheaper to replace budget and mid-range printers than to repair them.

5. Tackling hardware problems

Most crashes, errors and other problems are caused by software bugs, malware or security issues. Before you open up your computer, make sure you have eliminated other possible causes of the problem.

Consider calling in the experts

- Although desktop computers are generally designed so that some components can be replaced, it's often less hassle to call in your IT supplier.
- Laptops are best left to professionals and are often sealed by the manufacturer. They use custom components that are hard to access and soldered together to save space.
- Other devices - such as smartphones and tablets - are nearly impossible to repair. It's usually easier to get a replacement (under warranty, if you have one).

Many major components are relatively easy to replace in desktop computers

- For example, disk drives, power supplies, memory and so on.
- If your PC is outside its warranty, it is often more cost-effective to purchase a new one than to replace faulty components.
- If your computer is over a year old, it may be worth installing an upgraded component (eg a larger hard disk) instead of a direct replacement.
- Do not buy without a definite assurance that the new part will be compatible with your system.

It may be best to call in an expert to fix critical hardware

- They can provide a fast, guaranteed repair and peace of mind.

Upgrades can improve a computer's performance

- The main options are to upgrade the memory (RAM) and the hard drive.
- Adding more RAM can have a dramatic effect on system speed and should usually be your first step.
- If your computer uses a traditional magnetic hard drive that spins, you can replace it with a faster solid state model, also called an SSD. This can significantly improve loading times.
- These upgrades should only be attempted if you have experience working on computers. Components are easily damaged by static electricity.
- An upgrade may only buy you an extra year or so, making it more economical to replace the whole computer.

6. Troubleshooting software

Start by trying to replicate the problem

- Some software faults are caused by a particular combination of apps interacting poorly with one another. You may encounter a one-off problem purely by chance and never experience it again.

If you can replicate a fault, see if the software's help section offers a solution

The fastest way to find a solution is often to search online

- Check the manufacturer's website for help.
- If an error message is appearing, type that exact message into a search engine. You will probably find that someone has encountered the same problem before.
- Some firms offer online assistance. A support agent can remotely access your computer and fix the issue.
- Strange software behaviour may be caused by a virus or spyware. Always use up-to-date security software.

Manufacturers regularly issue software updates to fix bugs and security issues

- You should keep all your software updated.
- You can usually set software to download and install updates automatically.
- You may wish to test updates to critical software on a few computers before rolling them out across all company computers

You should usually aim to use the latest versions of software

- There may be specific reasons why you need to stick with an older version.
- Test new software on a few devices to ensure there are no bugs affecting you.
- Wait a few months after the release of new software before purchasing. This gives others time to find and iron out any bugs.

Remove unneeded applications properly

- Always use 'uninstall' or the option to 'add/remove' programs in the Control Panel. This should remove all traces of an application.

- Do not just delete the folder where the software is stored. This can cause problems by leaving files in different folders.

Signpost

- Find [Windows support](#) from Microsoft.
- Find guidance on [cyber security](#) from Get Safe Online.

Expert quotes

"Ensure you have a preferred list of IT suppliers and ask your staff to use them for all IT issues. This will reduce the risk of an employee asking a friend or family member for advice, and potentially causing expensive mistakes." - Bryan Archer, 3chillies

"Backing up to an external hard drive is a cost-effective and easy to manage strategy, especially when dealing with large volumes of data." - Paul Spearman, 3chillies

ACCA LEGAL NOTICE

This is a basic guide prepared by ACCA UK's Technical Advisory Service for members and their clients. It should not be used as a definitive guide, since individual circumstances may vary. Specific advice should be obtained, where necessary.

May 2018