THE ULTIMATE GUIDE TO IT SUPPORT WITH SuperFast IT

Everything you need to know about our services, contracts, costs and more
Contents

Introduction ............................................................................................................................................ 3

IT Support ............................................................................................................................................... 4
What is IT support? .................................................................................................................................. 4
What’s included with IT support at Superfast IT? ............................................................................... 4
Unlimited telephone, remote and on-site support ........................................................................ 4
24/7 System monitoring and remote remediation ......................................................................... 5
Multi-layered cyber protection ....................................................................................................... 5
Server backups and automatic offsite replication .......................................................................... 5
Email security protection ................................................................................................................ 5
Cyber security advice ...................................................................................................................... 6
Disaster recovery planning ............................................................................................................. 6
Strategic IT guidance ....................................................................................................................... 6

Cyber Security ......................................................................................................................................... 7
What are the risks? ............................................................................................................................. 7
Who will attack you? ........................................................................................................................... 8
How will they attack you? ................................................................................................................... 9
Untargeted attacks ............................................................................................................................. 9
Targeted attacks .................................................................................................................................. 10
12 Cyber security controls ................................................................................................................ 11
Cyber security training ...................................................................................................................... 12

Pricing and Contracts ........................................................................................................................... 13
Pricing ................................................................................................................................................ 13
Pricing Examples ............................................................................................................................... 14
Contracts ........................................................................................................................................... 15

Superfast IT Onboarding Process ..................................................................................................... 17
Discovery Session .............................................................................................................................. 18
Technology assessment .................................................................................................................... 18
You Visit Superfast IT ........................................................................................................................ 18
Onboarding You ................................................................................................................................ 19
Manage and Support ........................................................................................................................ 19

Contact Us ............................................................................................................................................. 20
Introduction

Welcome to the ultimate guide to IT support with Superfast IT.

Consider this guide everything you need to know about IT support as a service and how we provide it at Superfast IT.

Finding a new IT support company to provide a managed services agreement can seem a daunting task. At most, you’re likely to move once every three years meaning it’s crucial you get the decision right.

If you’ve downloaded this guide, it’s safe to say you’re after more information about IT support. This guide will cover everything from core services such as proactive and reactive support to pricing and contracts and everything in between.

Here at Superfast IT we have been supporting businesses and their technology for over 15 years.

We work with businesses with 10 to 100 employees, who need someone to take care of all their complicated technology.

We offer comprehensive IT management and support for a fixed monthly fee. Our managed IT support service operates 24/7* and includes unlimited support, remote monitoring and maintenance, server backups, computer security, and a dedicated account manager.

The service keeps your team working productively without disruption and frustration, enabling you to meet the needs of your customers.

Unlike the competition, we have both top-ranking customer satisfaction scores and super-fast response. Our outstanding service is all thanks to our treasured team of customer-caring IT experts and low staff turnover.

*24/7 support is an additional charge
**IT Support**

**What is IT support?**

In short, IT support is where a business like ourselves will provide you with technical support if you have a problem with technology in your business. If a user at your workplace has an issue with their computer, they can pick up the phone and call us. From here we can look to fix it remotely, or if that isn’t possible, we can visit your offices to fix the problem onsite.

Of course, this is just the very basic description of IT support, and it has many varying factors that we’ll look at in this section of the ultimate guide to IT support.

**What’s included with IT support at Superfast IT?**

There are several things included with IT support at Superfast IT. These range from reactive support and cyber security all the way to complimentary Superfast coasters.

Here’s a list of things included in our managed services package. We’ll describe each one in more detail and talk about how we provide the service at Superfast IT;

- Unlimited telephone, remote, and on-site support (we can also provide 24/7 support if required)
- 24/7 system monitoring and remote remediation
- Multi-layered cyber protection
- Server backups and automatic offsite replication
- Email security protection
- Cybersecurity advice
- Disaster recovery planning
- Strategic IT guidance

**Unlimited telephone, remote and on-site support**

Telephone support is the bread and butter of IT support. If you have a problem, you want to be able to pick up the phone and get it fixed. Most of the time IT issues can be solved remotely but for those that can’t you will need on-site support too.

This support should be quick and effective. If the problem is unable to be fixed remotely, there should be some form of on-site cover involved.

**Support with Superfast IT**

When we chose the name to Superfast IT, it became a promise to ourselves and our clients. We want to provide you with quick and efficient support to solve your problems.

Any problem you have is logged straight away and assigned a priority. If it’s a minor change, it won’t come before a business being down being unable to work. The tiered priority system means your problems get solved in a time span that’s acceptable to you.

We have a low staff turnover meaning you’ll be able to build up a working relationship with our friendly members of staff. You won’t get passed from person to person you’ll be dealt with and updated by the same person. If you call for an update on a problem, you’ll be able to speak to the person that’s working on it.
24/7 System monitoring and remote remediation

Your IT infrastructure is a 24/7 system. Updates or even malicious attacks can take place at any time during the day or night, so it’s important someone is always looking after your systems.

The better IT support companies utilise advanced monitoring tools to keep an eye on all aspects of your IT systems. These monitoring tools alert support staff in the event of pending/current issues, allowing them to take corrective action before users become aware of problems. Remote monitoring should take place 24/7, 365 days a year to provide you with the most uptime possible. Taking action in advance is also known as proactive support.

System Monitoring with Superfast IT

We’ll make sure that your systems get monitored 24/7 meaning you don’t have to worry. We want to know about a problem before you even know it exists. This monitoring also helps us identify faults or shortcomings in your IT infrastructure. We plan updates outside of your working hours to make sure there’s as little disruption as possible. How good would it be to call your IT support company about a problem to find out they’re already working on it?

Multi-layered cyber protection

Cyber security is no longer a choice it’s a necessity for every business. Your IT support company should provide you with several layers of protection for your data. They should make you aware of things such as two-factor authentication and password policies.

Cyber protection with Superfast IT

Cyber security is one of the most important things to us here at Superfast IT. That’s why this guide has a whole section dedicated to cyber security, which includes the 12 steps of protection we provide for your data.

Server backups and automatic offsite replication

In an ideal world, your data will get backed up several times a day. Not only this but it should be stored in at least one off-site location. If anything were to happen to your server or office, this means your data gets protected in a secure location. It should also be made clear to you where your data gets stored offsite.

Backups and offsite replication with Superfast IT

Your data is important to us. We’ll make sure your servers are backed up every single hour, meaning if you lose any data we should be able to get it back to you straight away. We also store your data in four different locations including offsite meaning if the worst were to happen to your offices we have a physical copy of your data safe and secure.

Email security protection

There are over 130 million phishing emails sent out every single day. Due to this, it’s more important than ever to protect yourself against spam emails. There are a number of ways to do this, and your IT support company should work closely with you to make sure you are protected.

There should be filters set up to make sure the malicious emails don’t even reach your inbox.

Email protection with Superfast IT
To protect your emails, we use an external service called ‘The Email Laundry’. Any email that you receive gets filtered through the service which will decide to quarantine it or not. This application stops hundreds of junk emails hitting your inbox every week. You’ll receive a daily report in your inbox highlighting any emails that have been quarantined. You can choose to release a specific email or whitelist a sender if you believe an email not to be spam.

**Cyber security advice**

Cyber Security can seem quite daunting to get your head around. That’s why it’s important for your IT support company to help you step by step with cyber security guidance. They should speak in a language you understand and explain how it will benefit your business.

**Cyber security advice with Superfast IT**

As previously mentioned cyber security is of the utmost importance to us here at Superfast IT. That’s why we’ll regularly sit down with you to see how you can improve your businesses’ cyber security and highlight risks. Rather than boring you with loads of jargon you don’t understand we’ll lay out the costs and benefits in a language you understand.

**Disaster recovery planning**

Nobody wants the worst to happen to their data or even their offices, but it is something that should be planned for. Working with your IT company your disaster recovery plan should be mapped out in case the worst happens.

**Disaster recovery with Superfast IT**

We’ll sit down with you to map out a disaster recovery plan for your business. We can then test this plan to make sure it works in case the worst happens to your business data. With our offsite backup offering we store your data securely in four different locations both on and off-site meaning we can always get your business back up and running again.

**Strategic IT guidance**

An IT company shouldn’t just answer the phone and fix your problems they should help your business grow through technology. Regular meetings with decision makers should be scheduled to talk about business and any recommendations that could improve your IT infrastructure.

**IT guidance with Superfast IT**

We want to be more than just a service to you; we want to create a successful business relationship. We’ll provide you with regular guidance on your IT infrastructure on how it can improve and make your business more successful. Our Strategic Business Reviews (SBRs) give us the chance to see how business is going and if you’re happy with the service.
Cyber Security

With a new cyber-attack or malware infection in the news almost every day, it can seem like a daunting task to protect your business. As the world becomes more connected by technology, cyber security has become a necessity, not a choice. Fortunately, we’re here to help.

At Superfast IT, we’ve been helping businesses with their cyber security for over 15 years. We’ve seen the cyber landscape change over those years as threats have become more sophisticated and complex.

- What are the Risks?
- Who will Attack you?
- How will they Attack you?
- 12 Cyber Security Controls

The first thing we want you to do is to think about your business. How big is your business? Does it have anything of value to a cyber-criminal? Are you cyber secure? What do you want to know about cyber security?

The more you know and understand about cyber security the more likely you are to protect yourself against it.

What are the risks?

By understanding the risks cyber-attacks can pose to your business it should encourage you to make sure your cyber security is the best possible. Even the most basic cyber security measures are now a necessity, or you will leave yourself open to these risks.

Here are 12 cyber security risks that could affect your business.

Leaking of sensitive company information

How much data does your company store? Client, employee and business-critical data are all at risk from inadequate cyber security. If this information got leaked into the public domain how much damage could it do to your business?

Malware infection

Poor cyber security on your network is an open gate for malware. Worms, viruses, ransomware and more will all cause problems for your business and could cause extended periods of downtime.

Attacks on your customers (using your systems)

What do you think your customers would say if your systems were used to launch a cyber-attack against them? Your systems could be used as part of a botnet attack if you have inadequate cyber security.

Damage or Defacement of your company resources

Your website is your first sales pitch to potential customers. Imagine if that was taken over by somebody looking to cause harm to your business reputation.
Unacceptable use of your systems

If cyber criminals get access to your systems, they could use it for several reasons. Not only could they damage your systems they could use yours to damage other people’s too.

Legal and regulatory sanction

Did you know poor cyber security can now get you fined? By not sufficiently protecting your clients’ data you run the risk of lawsuits, government fines and more.

Reputation damage

Some companies never recover from a cyber-attack. While they may be able to recover data and get systems back up and running the reputational damage can cause more harm than the attack. Customers can quickly lose trust in your business if you’re not protecting their data.

Financial loss through fraud

If somebody got full access to your systems how much money would be at their fingertips? Online fraud is on the rise, and it’s more important than ever to protect your company accounts.

Unauthorised changes to your systems

Cyber criminals can make changes to your systems without you knowing. Not only will these changes affect you in the short-term, but they can leave an ‘open gate’ on your network for them to visit any time they want.

Business disruption from security incidents

How much would one minute of downtime cost you? What about one hour? What about a whole month? Cyber-attacks can disrupt your business in several ways. Not only will you spend money fixing the attack you could be losing money from downtime at the same time.

Loss of data

Every record, document, file and more is always under threat from cyber-attacks. If you were to lose data due to weak cyber security, there’s a very slim chance you would ever see that data again.

Loss/theft of devices

If your device falls into the wrong hands would they be able to access your data? Make sure things such as two-factor authentication, secure passwords and the ability to remotely disable a device are implemented in your business.

Who will attack you?

When you think of hackers, you may imagine somebody sat in their bedroom having not seen sunlight for the last three days trying to breach a system. This couldn’t be further from reality. Cyber criminals are now part of organised groups with a vast amount of resources. They’re not the only people who could be attacking you; it may even be somebody in your office right now.

Cyber Criminals - Cyber criminals, are the likely suspects. They’re interested in making money through online fraud or the collection of valuable information.

Competitors - Competitors in both businesses and politics (Foreign Intel) will try to gain information to give themselves an economic or market advantage.
**Hackers** - Hackers will enjoy launching cyber-attacks. Hired for their hacking skills they’re experts at getting past network defences.

**Hacktivist** - Hacktivists, unlike hackers, will have a motive for their actions. The reasons often get based on politics or a company’s beliefs.

**Employees** - Not only employees but anybody who has legitimate access to your network. The attacks may happen on purpose out of spite against a company. Attacks can also occur on accident if a user doesn’t have the correct training.

**How will they attack you?**

**Untargeted vs targeted attacks**

In short, there are two types of attacks, untargeted and targeted. We’ll look at both with different examples of each type of attack.

**Untargeted attacks**

Untargeted attacks get massed produced without a real end goal in mind other than trying to hack into an unprotected system. Hackers will not target a set system/user they simply want to find unprotected accounts. They could do it for several reasons;

- Financial gain
- As a hobby
- Data collection

They will try to get into as many accounts at a time and keep repeating this process. Entry-level cyber security measures will block most of these attacks.

**Types of untargeted attacks**

**Phishing**

Phishing is your typical spam E-mail. Ever had an E-mail telling you, you’ve won a too good to be true prize or amount of money? That’s because it is too good to be true. They’re fake, they want your bank account details and should be deleted as soon as you get them. They can also tell you about ‘unusual activity’ on your accounts.

**Water Hole Attacks**

Water holing attacks are the act of setting up a fake website that looks very similar to its real-life counterpart. The sites usually are online E-commerce sites such as Amazon or PayPal that people regularly use with their bank account details. At times the previously mentioned phishing leads to water holing. Once people visit and use these sites, the hackers will have the information sent to them leaving the user vulnerable to cyber-attacks or money fraud.

**Ransomware**

This mass attack will infect vulnerable systems before locking the user out of the accounts. The hacker can then demand money or more information before they give access back to the account.

**Scanning**
Scanning tends to be the attack that has the lowest hit rate as it just searches the internet at random. There’s no set direction for the attack as it scans broad areas of the web looking for unprotected accounts.

**Targeted attacks**

Targeted attacks target a particular thing such as a specific network or user. The attack could get aimed at an individual user or an entire business. The hacker may have numerous reasons for carrying out the attack;

- Personal Grudges
- Rival company
- Been paid to target you

These take much longer to execute than untargeted attacks and can even take months or years to set up depending on the scale of the attack. The majority of these attacks use bespoke capabilities and often go undiscovered even after the attack.

**Types of targeted attacks**

**Spear phishing**

It follows the same guidelines as the previously mentioned phishing except rather than being mass produced. It will target an individual or a company containing specific attachments that appeal to the recipient of the E-mail.

Imagine two people fishing at a pool. A fisherman (phishing) would try to catch any fish in the pool. Meanwhile, a spear-fisher (spear-phishing) would target a singled-out fish.

**Deploying botnets**

When a hacker uses a botnet, it will flood the bandwidth of a targeted system(s) with an overload of traffic from multiple sources making the online service unavailable. Attackers build up a network of infected computers then use them to attack a targeted system(s) at the same time.

**Supply chain**

Subverting a supply chain is probably one of the hardest ways for a hacker to get access. They try to get their hands-on equipment or software that is being delivered to an organisation and infect it before installation.

**Insider threats**

People inside your workplace can be the biggest threat to your business. They can have the account passwords and access to several sources of information that should be kept private.

Workers could have been paid by a third-party source to gather information for them or could do it out of personal spite. They will know how the system works, so it is worth the hackers’ money paying for somebody who is on the inside.
12 Cyber security controls
To help you put in place robust cyber security defences without breaking the bank, we’ve brought together 12 primary security controls, based on guidance from the UK Government’s National Cyber Security Centre, which include those incorporated within the Cyber Essentials framework.

Network Perimeter Defences
Network perimeter defences will block any external attacks on your network keeping your data safe. With 1.9 billion records lost or stolen in the first six months of 2017, this is a critical part of business cyber security.

Secure Configuration
Secure configuration refers to security measures that get implemented when building and installing computers and network devices to reduce unnecessary cyber vulnerabilities.

Software Patching
Is your software up to date? If it’s not, it’s a major security risk. You only have to look at the WannaCry ransomware in May 2017 to see the damage that can be caused on unprotected or unpatched software.

User Account Control
Allowing employees access to all your data is a major security risk. Make sure each user only has access to what they need. If a user leaves or moves department, make sure the access gets revoked.

Malware Protection
Malware is an umbrella term for anything bad on your computers such as viruses and ransomware. Malware protection will help guard you against dangers online that could infect your devices.

Backing up your data
When was the last time you backed up your data? Last week? Last month? Last year? Never? You
should be taking a regular backup of your data with active copies to access and store them in a safe place.

**User education & awareness**

Cyber security is for everybody in an organisation, not just a few people. Your network will only be as secure as your weakest link. Make sure everybody has had the correct cyber security training and is aware the company protocols.

**Email protection**

Spam protection on your email inbox can help guard against phishing attempts. With 156 MILLION phishing emails sent per day, it’s more important than ever to protect your email accounts.

**Block malicious websites**

There are thousands of malicious websites online, and some are easier to spot than others. Take away the risk of these websites by blocking access to them all together.

**Removeable media controls**

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

**Secure Wi-Fi**

Do you know who has access to your Wi-Fi? Do you have a list of devices that connect to your Wi-Fi? Is there a secure password on the router? A poorly secure router is an open gate to your network.

**Security monitoring**

Dedicate somebody to make sure everybody has the right protection and are following the correct procedures when it comes to cyber security.

**Cyber security training**

To help improve the cyber security in your business we can provide you with tailored cyber security training for your staff.

We can come into your offices and present a cyber security presentation highlighting common dangers to look out for in day to day work.

Before the presentation, we can send out fake scam emails to see which members in your organisation are getting caught out. This can be an ongoing process to make sure people are learning and are not continuously falling for scam emails which could put your business at risk.
Pricing and Contracts

When choosing an IT support provider one of the main factors that will affect your decision will be the price. Every IT company will have a different pricing model, so it’s important you get full clarification before signing any agreements. Contracts are also important, and there are several things to look out for that we’ll discuss in this section.

Pricing

The cost of a managed services agreements is often one of the overriding factors when deciding which company to choose. It can be easy to go for the cheapest offer on the table, but this usually means a compromise on the quality of service. There is a wide range of factors that can affect the price of an agreement. These factors can include numbers of users, servers, hardware, applications and more.

Pricing at Superfast IT

At Superfast IT we want to be open and honest with you about our prices. There are no hidden extras, and we make our pricing available to see on our website. Lots of other IT companies will tell you they’re the ‘cheapest’ but force you to get in touch before you can find out any pricing information. A managed services agreement with Superfast IT is made up of four key components. Of course, there can be additions for other things such as project work and new technology, but these four services are the main bulk of your cost.

Desktop Secure - £2.95 per computer, per month

Your security while using your computer is of the highest importance to us. Desktop Secure for just £2.95 per month allows us to protect your data. It provides anti-virus and malware protection, security monitoring and patching as well as domain name filtering. It’s the all in one tool for protecting you and your data.

Virtual IT Department - £25 per user, per month in your business

The virtual IT department will provide you with unlimited business remote support during our working hours (8am-5pm). If you have a problem, pick up the phone and ring our service desk and we’ll get to looking at your problem straight away. If the problem is unable to be fixed remotely, this cost also covers support on your site for more complex problems.

If you need 24/7 support, we can provide this at an additional cost.

ServerCare - £49 per server per month in your business

ServerCare, as the name suggests, looks after the servers in your business. The software includes 24/7 monitoring as standard which will alert us to any issues before you even know you have them. We can also remotely apply updates and security patches outside your working hours to give you the least disruption possible.

Offsite backup – 1tb = £100 per month

Could you afford to lose your business data? Our offsite backup plan makes sure you will always be able to access your data if the worst happens. We take regular backups throughout the day, so you will always have access to your latest documents if the worst happens. The data is then stored in four different locations to help protect against the unlikely cause of natural disasters.
Pricing Examples

- **10 User Business**
  - 1 Server
  - 1TB Offsite Backup
  - Desktop Secure £2.95*10, per month
  - Total = £29.50
  - ServerCare £49*1, per month
  - Total = £49

  **Offsite Backup** £100*1, per month
  - Total = £100

- **25 User Business**
  - 1 Server
  - 2TB Offsite Backup
  - Desktop Secure £2.95*25, per month
  - Total = £73.75
  - ServerCare £49*1, per month
  - Total = £49

  **Offsite Backup** £100*2, per month
  - Total = £200

  **Virtual IT Department** £25*10, per month
  - Total = £250

- **50 User Business**
  - 2 Servers
  - 4TB Offsite Backup
  - Desktop Secure £2.95*50, per month
  - Total = £147.50
  - ServerCare £49*2, per month
  - Total = £98

  **Offsite Backup** £100*4, per month
  - Total = £400

  **Virtual IT Department** £25*50, per month
  - Total = £1250

**Total**
- **Circa £430** Per Month
- **Circa £950** Per Month
- **Circa £1900** Per Month
While at first glance you may think this seems expensive when you look at the value it adds to your business, it can become a very valuable service. Especially compared to an internal IT team. At Superfast IT the above prices will include all the following:

- Unlimited telephone, remote, and on-site support (During our business hours)
- 24/7 system monitoring and remote remediation
- Multi-layered cyber protection
- Hourly server backups and automatic offsite replication
- Email security protection
- Cybersecurity advice
- Disaster recovery planning
- Strategic IT guidance

As previously mentioned this is a much more cost-effective way than insourcing your own IT team. The average wage of a senior IT technician is circa £25,000. If you hired someone on this wage, it would cost you over £2000 a month, and this doesn’t take into account, holidays, sickness, training and a host of other things.

Contracts

Not only is the price you pay important but the details of the contract too. Many IT companies will look to tie you into long seemingly never-ending contacts. You should try to avoid this at all costs as they will charge you an extortionate fee to leave your agreement early.

Before signing anything, you should make sure you know what’s included, here are a few things to look out for;

Payments – How and when will you pay for the services? Most companies will send you an invoice monthly that must be paid within a certain time. You may also have to pay the first month upfront when you sign an agreement.

Length of contract – As previously mentioned many IT companies will look to tie you into long contracts that are impossible to escape. On the other hand, some companies will have monthly rolling contracts. It’s important to know how long you’re signing into an agreement.

Notice period – If for some reason you want to leave your contract early it’s worth knowing how long your notice period will be. Some companies will allow you to leave straight away while some will make you sit out the remainder of your contract.
**Hours of cover** – What hours of cover will the IT company be able to provide you? Do these match up with your business hours? Some companies will open your basic 9-5 hours while others will offer 24/7 support. Make sure you know when support is available before you sign up.

**Any additional costs** – Not everything gets included in the monthly payments in your contract, and it’s important to know what is and isn’t. Usually, support will get included, but things such as additional software and projects will come at an extra cost.

**Contracts at Superfast IT**

At Superfast IT we won’t tie you down into long contracts that seem impossible to escape. All our contracts are on a monthly rolling basis with a months’ notice period. The monthly rolling contract means you’re free to leave at any time and aren’t tied into a long-term commitment.

If for some reason that doesn’t suit your business, we can also provide you with a contract length of your choice such as one to three years fixed contract. All our invoices are billed monthly.

Our support helpline is open from 8am-5pm Monday to Friday, excluding bank holidays. For an additional cost, we can provide a 24/7/365 support contract if that suits your business better.

Just like our pricing we want to be open and honest with you.
Superfast IT Onboarding Process

- Discovery Session
- Technology Assessment
- You Visit Superfast IT
- Onboarding You
- Manage & Support
Moving to a new IT support company can seem a daunting task. It’s not something you often do, so you want to make sure you get the decision right. One of the biggest worries people have when moving managed service providers is the onboarding process such as how long it will take and if there are any hidden costs.

Here at Superfast IT, we want to be open and honest with you. This section will document our onboarding process with any costs involved making it clear for you.

**Discovery Session**
The first point of contact between ourselves and a potential client will be a discovery session. This meet can take place in person or over the phone. It’s our way of distinguishing how we can help you and the role IT plays in your business. We can look at your business goals to see where you aim to be and any current issues you’re currently facing with technology in your business.

**Technology assessment**
The next step in the process of our onboarding is a technology assessment. One of our engineers will come to your offices and assess your network. We’ll look at things such as the number of users, servers amongst any other technology in your business. The assessment also gives you the opportunity to talk about any specific applications or hardware you have in your business that we will need to look after.

A technology assessment from Superfast IT costs £250. Just because you have a technology assessment doesn’t mean you 100% have to go forward with a managed services agreement.

**You Visit Superfast IT**
After the technology assessment, we’ll invite you into our office for an informal chat over a cup of coffee. The meeting allows us to discuss what we found in the prior assessment such as risks to your business and give you details of the contract for a managed services agreement.

All our contracts are on a monthly rolling agreement with a 30-day notice period, so you’re never tied into a long contract. For more information on our pricing and contracts check out our pricing page.

We’ll walk you step by step through the contract and price for each part of our service. We can make any revisions and answer any questions at this time too. It also gives you the chance to meet our team here at Superfast IT and see how they’ll help benefit you.

If you coming to our office doesn't quite suit you we can always have a chat in your office. But we find it a great opportunity for you to see what we're all about and meet our employees.
We won’t push you for your signature there, and then, if you need time to go away and discuss with others before signing it off, that’s fine with us.

Onboarding You

Once the contract has been signed off, we can start getting you onboarded and becoming one of our clients. Even if everything isn’t quite in place, you’re still free to call us, and we can start offering support straight away.

There will be several visits to your office during this period to get everything set up and working. These visits will be of no additional cost to you.

Manage and Support

You’ve had the technology assessment; you’ve come into our office for a chat, we’ve got you set up and onboarded so what’s next? Well our IT support comes with a host of things to take your IT headaches away and help your business run smoothly.

• Unlimited telephone, remote, and on-site support (we can also provide 24/7 support if required)
• 24/7 system monitoring and remote remediation
• Multi-layered cyber protection
• Hourly server backups and automatic offsite replication
• Email security protection
• Cybersecurity advice
• Disaster recovery planning
• Strategic IT guidance

As part of your ongoing support, you’ll get a dedicated account manager who you will talk to through regular meetings. The purpose of these meetings is to see how business is going for you and see if there have been any changes over the last few months. They’ll also be in regular contact with you through the Quarterly Business Reviews we carry out.
Contact Us
We hope this guide has given you a good idea of what to expect from an IT support company and how we do things at Superfast IT. Want to know more? Have any questions? Want to come in for an informal chat and a coffee? Feel free to contact us.

Website – Superfast-it.com

Telephone – 0121 309 0090

Office location - Suite 2, Winwood Court
Norton Road
Stourbridge
West Midlands
DY8 2AE

Social media;
Twitter - @SuperfastIT
Facebook - /SuperfastIT
LinkedIn – Search for Superfast IT