

— THE BUYER'S GUIDE

How to choose the right IT support provider

A straightforward guide for small businesses that are new to managed IT, or quietly thinking about switching.



Martin Robinson
Founder, Adoptive Technologies

Before you start

Choosing an IT provider is harder than it should be.

There is no regulator, no qualification you can check at the door, and almost every provider says the same things on their website: proactive, responsive, secure. This guide is here to help you see past that.

Whether you have never had proper IT support, or you are quietly fed up with the provider you have, it explains what a good service includes, what to ask before you sign anything, and how to spot the warning signs.

I have also been honest about the trade-offs between a small, founder-led provider like Adoptive and a larger one. You are better off choosing well than choosing us by default, and a good provider will happily answer every question in this guide.

If anything here raises a question, pick up the phone. I would rather talk it through.



Martin Robinson

Founder, Adoptive Technologies
01329 759777

Inside this guide

Why use an IT partner?	3
What a managed service includes	4
Signs it might be time to switch	5
Ten questions to ask	6
Pricing and contracts	8
Small or large provider?	9
Security basics	10
Switching without the drama	11
Provider scorecard	12
How Adoptive answers	13
Talk to us	14

How to use this guide

Read it end to end, or jump to what you need. Comparing providers? Start with the questions on page 6 and the scorecard on page 12. Not sure whether to leave your current one? Page 5 is a good place to begin. Everything here applies whoever you end up choosing.

Why use an IT partner?

A good IT partner does far more than fix things when they break. Here is what you should expect to gain.

1 Fewer surprises

Monitoring spots problems early, so many are fixed before your team has even noticed something is wrong.

2 Predictable costs

A clear monthly price replaces unpredictable call-out bills, which makes IT far easier to budget for.

3 Planning, not just repairs

A view of what is ageing and when it needs replacing, so equipment is planned for rather than panic-bought.

4 Wider know-how

No single employee can be an expert in email, security, networks and licensing. A good partner brings that breadth, or knows who to call.

5 Cover when you need it

Holidays, sickness and busy periods stop being a worry when support does not depend on one person's diary.

6 Security taken seriously

Backups, updates and account protection are handled as a standing routine, not something remembered after an incident.

7 Honest licensing advice

Someone who checks what you are paying for, and tells you when you are paying for things you do not use.

8 A sounding board

Someone to ask the bigger questions: should we move, should we replace this, is that email a scam?

Is outsourcing always the answer?

Not always. If you already have a capable in-house IT person, the best arrangement is often co-managed: they keep the day-to-day, and an outside partner covers holidays, specialist projects and security. A good provider will say so, rather than trying to replace someone who is doing a good job.

What a managed service should include

"Managed IT" can mean very different things from one provider to the next. Use this as a checklist when you compare what is on offer.

SERVICE	WHAT IT MEANS IN PRACTICE	WHAT TO LOOK FOR
Support when things go wrong	A clear way to report problems and get help from someone who knows your setup.	Agreed response times in writing, and a record of every request.
Monitoring	Your devices and systems are watched continuously for faults, failing disks and security warnings.	Round-the-clock monitoring, with a clear answer to "who sees the alerts?"
Updates and patching	Security fixes and software updates are applied regularly, not left for months.	A routine that includes testing, and a plan for out-of-hours work.
Backup and recovery	Copies of your important data kept separately, including cloud services like Microsoft 365.	Regular test restores. A backup nobody has tested is only a hope.
Security	Multi-factor authentication, protection on every device, email protection and sensible admin controls.	A recognised baseline such as Cyber Essentials, explained in plain English.
Asset records	An up-to-date list of devices, licences and renewal dates.	Proactive reminders before warranties and licences expire.
Starters and leavers	New staff set up properly and leavers' access removed promptly.	A defined process, not a favour you have to request each time.
Documentation	Your setup written down: accounts, systems, suppliers and how it all fits together.	You should be able to see it, and it should leave with you if you switch.
Reviews and planning	Regular conversations about what is working, what is ageing and what is coming.	A simple roadmap and budget view, not just a list of tickets.

A useful test

If your provider only ever appears when something has broken, you have a repair service, not a managed one. **Managed means someone is looking after things in between the problems.**

Signs it might be time to switch

Most businesses put up with disappointing IT support for far longer than they should, because changing feels like hard work. These are the signs worth taking seriously.

1

You are always the one chasing

You notice the problem, you report it, and then you chase for an update. Good support works the other way round.

2

Response times have quietly slipped

What used to take an hour now takes half a day, and because nothing was ever agreed in writing there is nothing to point to.

3

The same problems keep coming back

A quick fix every time, but nobody asks why it keeps happening. Repeat faults should lead to a root-cause fix.

4

You only hear from them when something breaks

No check-ins, no planning conversation, no view of what is coming up. That is reactive support.

5

Jargon instead of answers

If you leave every conversation less sure than you went in, something is wrong. You should always understand what is being done and why.

6

Security feels like an afterthought

It only comes up after an incident, or in the form of a scary sales pitch, rather than as a steady part of how things are run.

7

Every conversation ends in a quote

New kit has its place, but a good provider helps you get the most from what you have before suggesting you replace it.

8

You are not sure who would pick up in an emergency

If you could not say who you would call at 8am on a bad day, or whether they would answer, that is worth fixing.

One or two of these is a conversation worth having with your current provider first. **Three or more** is a pattern, and it is probably time to look around.

Ten questions to ask any provider

Anyone can set up as an IT provider, so asking good questions matters. For each one, here is what a strong answer sounds like and what should make you pause.

1 What happens when I report a problem?

A GOOD ANSWER

A clear route in (phone, email or portal), every request logged, and agreed response times that are written down.

A RED FLAG

"Just give us a call." No record, no timings, and no way to see what has been done.

2 How do you stop problems happening in the first place?

A GOOD ANSWER

Continuous monitoring, regular updates, and a habit of finding out why a fault keeps recurring rather than just resetting it.

A RED FLAG

The honest answer is "we wait for you to tell us". That is a repair service, not a managed one.

3 Who will actually look after us, and who covers when they are away?

A GOOD ANSWER

Named people, and a straightforward explanation of how holidays, sickness and out-of-hours issues are covered.

A RED FLAG

"The team will look after you" with no names, or no clear answer about what happens when your contact is unavailable.

4 How is our data protected?

A GOOD ANSWER

Separate backups (including Microsoft 365, which Microsoft does not back up for you), multi-factor authentication, tested restores and a recognised standard such as Cyber Essentials.

A RED FLAG

They cannot tell you when a backup was last tested, or they treat security as an optional extra.

5 What is included in the price, and what is not?

A GOOD ANSWER

A written scope, a simple price per user or per device, and a plain list of what costs extra.

A RED FLAG

A low headline price with a long list of "out of scope" items that turn out to be the things you actually need.

Questions 6 to 10

These cover the commitment you are making, and whether the relationship will last.

6 How long is the contract, and how do I leave?

A GOOD ANSWER

A sensible term, a clear notice period, and a written exit process that includes handing over passwords and documentation.

A RED FLAG

A long term that renews automatically, or an awkward answer when you ask what happens if you want to go.

7 Will you help us plan, or only fix things?

A GOOD ANSWER

Regular conversations about what is ageing, what is coming up and what it will cost, ideally in a simple roadmap.

A RED FLAG

Planning only happens when there is something to sell you.

8 Do you work with businesses like ours?

A GOOD ANSWER

Specific examples from your sector or size, and confidence with the software and devices you use, whether that is Windows, Mac or something specialist.

A RED FLAG

A generic pitch that could be for anyone, or hesitation about your particular set-up.

9 How will you explain things to us?

A GOOD ANSWER

Plain English, in whatever form suits you, with an offer to explain anything twice.

A RED FLAG

Jargon in the sales conversation. If it is confusing before you sign, it will be confusing afterwards.

10 Can I speak to some of your customers?

A GOOD ANSWER

"Of course." References, or at the very least reviews you can read for yourself.

A RED FLAG

Reluctance, or only ever one glowing quote that cannot be traced to a real business.

Worth asking as well: How does your team stay up to date? Will my staff get training on the tools we pay for? Can I see how well the service is performing?

Pricing and contracts

The cheapest price on paper is rarely the cheapest service in practice. Here is how to compare like with like.

HOW PROVIDERS CHARGE	HOW IT WORKS	WORTH KNOWING
Per user	A fixed monthly amount for each person in your business.	Easy to budget for and easy to scale. Check what happens when staff numbers change.
Per device	A monthly amount for each computer, server or device covered.	Can suit businesses with shared machines. Check whether phones and tablets count.
Tiered bundles	Packages (basic, standard, premium) with set features.	Read exactly what sits in each tier. The feature you need is often in the top one.
Pay as you go	You are billed for the time spent on each job.	Flexible, but nobody has a reason to stop problems recurring, and costs are unpredictable.

Things that catch people out

Software licences billed separately from the service.

Onboarding or set-up fees that were not mentioned up front.

Charges for out-of-hours help, or for projects such as moves and migrations.

Price increases partway through a term, or on renewal.

Backup and security quoted as optional extras.

Before you sign, check

The length of the term, and the notice period needed to leave.

Whether the contract renews automatically, and when you would need to act.

How and when prices can change.

That you own your data, domain and admin accounts, and that these are handed over if you leave.

What the response times are, and what happens if they are missed.

Ask for a worked example

Ask each provider to quote for your actual business: your number of staff, your devices, and the services you have told them you need. **A quote you can add up yourself, with nothing left vague, is a good sign.**

Small provider or large provider?

Neither is automatically better. They suit different businesses, and each has weak spots you should ask about.

Smaller, founder-led

One person or a small team

WHERE IT SHINES

- The same person every time, who already knows your setup
- A direct line, with no queue or middle layer
- Flexible, personal and quick to act
- You matter to them

QUESTIONS TO ASK

- What happens if you are ill or on holiday?
- Who do you call for specialist issues?
- Can you cope if I grow quickly?

Larger, multi-team

A service desk and account managers

WHERE IT SHINES

- Depth of specialist skills in one place
- Cover is built in
- Formal processes and escalation routes
- Capacity for large projects

QUESTIONS TO ASK

- Will I get the same people each time?
- How quickly do I reach someone who can actually fix it?
- Will a business my size get proper attention?

Whichever you choose, ask these five

- ☐ **What happens if you are unavailable?** There should be a clear, honest answer, not reassurance.
- ☐ **Where is our documentation kept?** You should be able to see it, and it should be yours.
- ☐ **Is there emergency access to our systems?** At least two administrators, so one lost phone cannot lock you out.
- ☐ **Who watches for problems out of hours?** Monitoring should not depend on someone being at their desk.
- ☐ **Who do you bring in for what you cannot do yourself?** Every provider has limits. The good ones are open about them.

There is no wrong size, only the wrong fit

A founder-led provider suits a business that values knowing exactly who it is dealing with. A larger one can suit a business that needs many hands for big projects. **Choose for your situation, then put the five questions above to whoever you are considering.**

Security basics any provider should cover

You do not need to become a security expert, but you do need a provider who handles the basics properly. "We take security very seriously" costs nothing to say, so ask to see the evidence.

THE BASIC	WHY IT MATTERS
Multi-factor authentication	A stolen password on its own should not be enough to get into email or files. This matters most on administrator accounts.
More than one administrator	If the only person who can manage your Microsoft 365 account loses their phone, you can be locked out of your own email. A secure backup route in is essential.
Backups that are tested	Including cloud data such as Microsoft 365. Ask when a restore was last tested, and how long it took.
Updates and patching	Most attacks use weaknesses that already have a fix available. Staying current closes those doors.
Email protection	Properly configured email records (SPF, DKIM and DMARC) make it harder for criminals to send messages that look like yours.
Protection on every device	Up-to-date security software and sensible limits on who can install things.
Staff awareness	People are often the weakest link, and the best defence. Short, regular training beats a once-a-year lecture.
A recognised standard	Cyber Essentials is a government-backed scheme covering the core controls. It gives you something concrete to ask a provider about, and to hold them to.

Five things you can check this week, whoever your provider is

- ☐ Does every account with administrator rights use multi-factor authentication?
- ☐ Can you name at least two people who can administer your Microsoft 365 account?
- ☐ Do you know when a backup was last test-restored, and by whom?
- ☐ Is every device in the business receiving updates?
- ☐ Could you find your IT documentation today if you needed it?

You can also check your email domain's SPF, DKIM and DMARC records for free at adoptivetechologies.co.uk/email-analyzer.

Switching without the drama

Changing provider sounds like a big project, but a well-run handover should be quietly unremarkable. Here is roughly what to expect.

01

Talk it through

A review of your current set-up and what is frustrating you, so the new provider starts with the real picture.

02

Handover preparation

An introduction to your outgoing provider where possible, and the key information gathered: access, accounts and documentation.

03

Plan the changeover

Agreed dates, with any disruptive work scheduled out of hours so your team carries on as normal.

04

Set up the essentials

Monitoring, backup and security put in place so protection is running from day one.

05

Bring your team along

Staff know who to contact and how, and what, if anything, will look different.

06

Review after a month

A check that everything is working well, and a chance to raise anything that was missed. Many moves take around 30 days from start to finish.

Gather before you start

Admin logins for Microsoft 365 and any other key services.

Access to your domain name and website hosting.

A list of software, licences and renewal dates.

Warranty and supplier details for key equipment.

Check your contract first

Look up the end date and the notice period before you tell anyone.

Some contracts renew automatically if notice is missed.

Ask what your current provider has to hand over, and by when.

Be patient with staff: new systems take a little getting used to.

Your new provider should do the heavy lifting

You should not have to manage your own migration. If a provider expects you to coordinate the handover yourself, ask how many they have done, and what usually goes wrong.

Provider scorecard

Print this page and score each provider you speak to. Add up the totals, but trust your gut too: how a provider makes you feel in the first conversation usually tells you a lot.

2 clear yes, in writing 1 partly, or vague 0 no, or no answer

QUESTION	PROVIDER A	PROVIDER B	PROVIDER C
Response times agreed in writing Not just "we're quick"			
Proactive monitoring included Someone is watching between problems			
Named people, and clear cover You know who, and what happens when they are away			
Backups tested, including Microsoft 365 They can tell you when a restore was last tested			
Security approach and recognised standard For example Cyber Essentials			
Clear pricing you can add up Including what is not included			
Fair contract and clear exit terms Notice period, renewal, handover			
Explains things in plain English How did the first conversation feel?			
Experience with businesses like yours Sector, size and software			
Happy to give references or reviews Real customers you can check			
Total (out of 20)			

How Adoptive answers these questions

You should hold us to the same standard as everyone else. Here is how we would answer the questions in this guide.

YOU ASK	HOW WE ANSWER
What happens when I report a problem?	Issues are picked up, worked through and closed with the wider business in mind, not just the ticket. We work to assigned response times, so you always know when help is on its way.
How do you prevent problems?	Monitoring is how problems get caught early, and round-the-clock (24/7) monitoring is available as an optional add-on. Either way, when something keeps coming back we fix the root cause rather than patching it again.
Who looks after us?	You deal directly with me, the same person every time, who already knows your setup. If I am ever away I will be upfront about when I am back. We are founder-led, happy to talk openly about what that means in practice, and 24/7 cover is available as an optional extra.
How is our data protected?	We are Cyber Essentials certified, and the protection we put in place for clients is aligned to the same standard. Dark web and threat monitoring is part of our cyber security service, and independent Microsoft 365 backup with regular recovery testing is an optional add-on.
What does it cost?	From £40 per person per month (ex VAT), fixed and transparent. Backup and disaster recovery and 24/7 monitoring and support are optional add-ons, and Microsoft 365 licences are sold separately.
Will you help us plan?	Yes. Strategic IT roadmaps, support through projects and migrations, and honest vendor and licensing advice, so you stop paying for what you do not need.
Do you know our sector?	We work with accountants, engineering firms, architects, and education and training providers, among other established small businesses.
How do you handle a switch?	Carefully, with minimal disruption. Most onboards take around 30 days, and we ask for an introduction to your current provider so the handover is smooth.

Included in the monthly price

- Fully managed IT support from a UK-based team
- Cyber security aligned with Cyber Essentials
- Microsoft 365 management and monitoring
- Virus and ransomware protection for your computer

Optional add-ons

- Backup and disaster recovery
- 24/7 monitoring and support, with round-the-clock cover rather than just business hours

Microsoft 365 licences are sold separately.

TALK TO US

Let's have a conversation, with no pressure

If this guide has helped, we would be glad to talk about your business. A complimentary call takes around 15 to 20 minutes, and you will speak to a real, named person, usually me.

- ✓ We ask about your business and what is frustrating you
- ✓ We talk honestly about whether we are the right fit
- ✓ No jargon, no pressure and no obligation

BOOK A CALL

adoptivetechologies.co.uk/contact

Choose a time that suits you

CALL US

01329 759777

Straight through to a real person



Adoptive Technologies Limited | Merlin House, 4 Meteor Way, Lee-On-The-Solent, Hampshire, PO13 9FU
Registered in England and Wales, company number 15948413