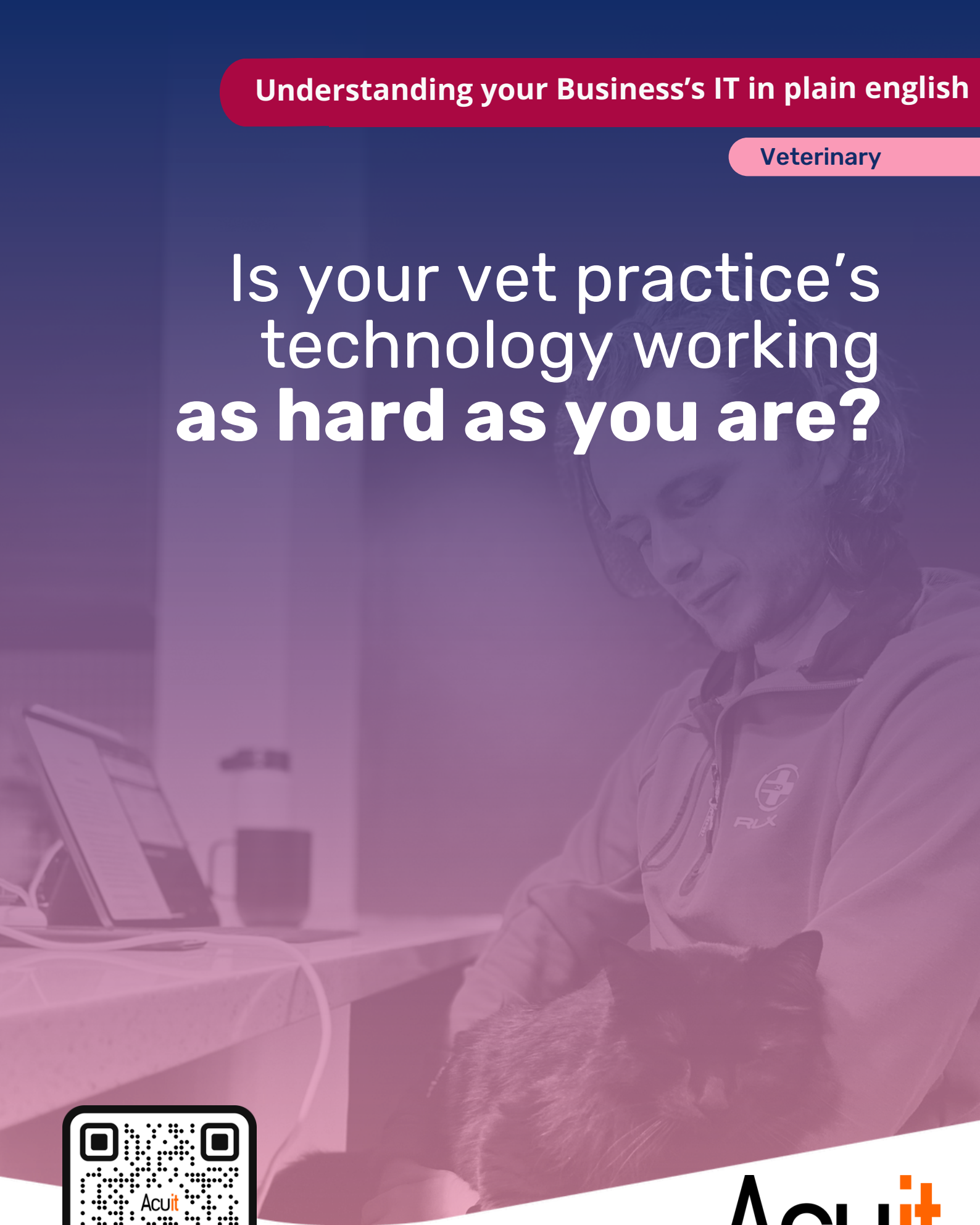
Understanding your Business's IT in plain english

Veterinary

Is your vet practice's technology working **as hard as you are?**



SCAN ME

Acuit

0141 255 1617

By 8am, the phones are already ringing.

The operating theatre has been prepped since seven.

The waiting room is filling up. Someone's dog is anxious. A nurse is dealing with a message about last night's out-of-hours call.

In that environment, nobody stops to wonder whether last night's backup ran, whether the Wi-Fi is set up properly, or whether the software running the practice is years out of date.

Those questions tend to surface at the worst possible moment.

Like on a packed Saturday morning. Or in the middle of a procedure. Or when you're trying to access records for an animal that's just been brought in.

The good news is that you don't need to understand technology deeply to make good decisions about it.

You simply need to know the right questions to ask, have a basic picture of what your systems are doing, and have someone you trust looking after the parts you can't see.

Awareness, plus the right support, is what separates practices that handle technology problems well from those that get caught out by them.

Why technology matters **more in a vet practice**

Vet practices are unusual businesses.

On any given day you're running a clinical environment, a retail operation, a service for anxious pet owners, and something that can function as an emergency facility.

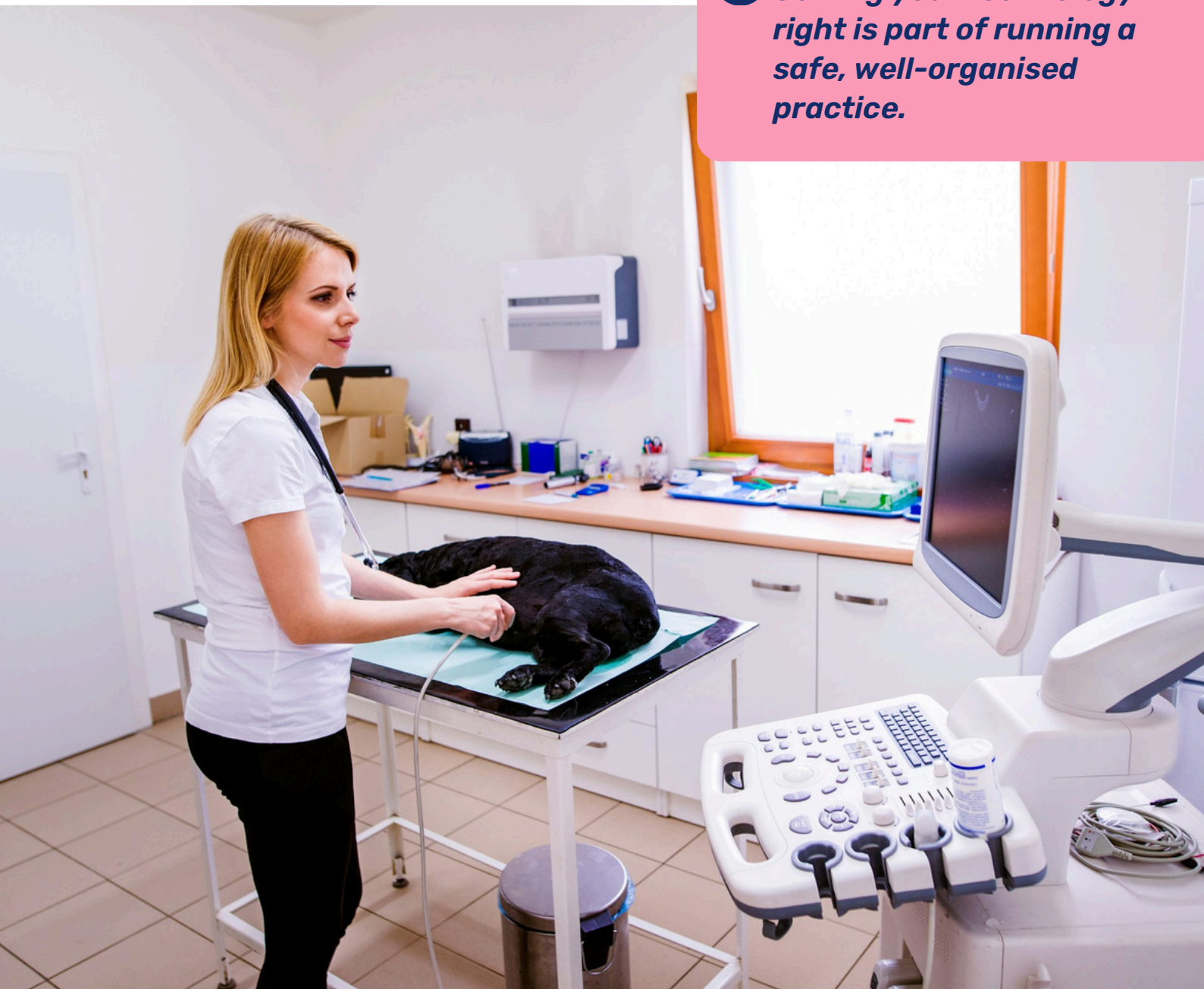
Other businesses may be only one of those things. Yours is all of them at once.

That means when something goes wrong with your technology, the consequences are very different from what they would be in a typical office.

A slow system during morning consultations backs up the entire day.

A problem with your appointment records on a busy Saturday creates gaps in patient histories, adds pressure to an already stretched team, and in serious cases can affect the care animals receive.

Getting your technology right is part of running a safe, well-organised practice.



Do you know **what you've got?**

Many practice owners assume their technology is working because nothing has gone visibly wrong.

That's a different thing from *knowing* it's working.

It's worth asking yourself a few honest questions.

Do you know where your patient records are physically stored?

Are they on a server inside the building, or on a remote system accessed over the internet (what's usually called "the cloud")?

Do you know who is responsible for backing them up, and when someone last checked that those backups work?

A backup that runs every night but has never been tested isn't really a safety net.

If your practice management software went down right now, what would happen to this morning's schedule?

Is there a written plan for that kind of situation? And would your team know where to find it?

Another common question involves personal devices.

How many staff phones, home laptops, or personal tablets are being used to access practice systems?

This is far more common than most practice owners realise. Each device is another possible way in for someone who shouldn't have access.

These questions can feel uncomfortable, but that discomfort is useful. It highlights the gap between assuming everything is fine and knowing that it is.

The security risks that are **specific to vet practices**

Cyber attacks on small businesses aren't random.

Criminals actively look for organisations that hold valuable data, use older software, and don't have a dedicated IT team watching for threats.

Vet practices often fit that description.

If someone gained unauthorised access to your practice management system, they would have access to a lot of data.

Busy clinical environments also create a particular vulnerability.

When a critical patient arrives and everyone is moving quickly, people make decisions faster than usual.

A suspicious email that might normally be spotted gets opened. A login page that looks familiar gets used without a second thought.

Some cyber criminals deliberately target busy workplaces for exactly this reason.

Another common issue is outdated software.

Many practices continue running systems that haven't been updated in years because changing them feels disruptive.

Unfortunately, older software often contains known security weaknesses.

Once those weaknesses become public knowledge, attackers know exactly where to look.

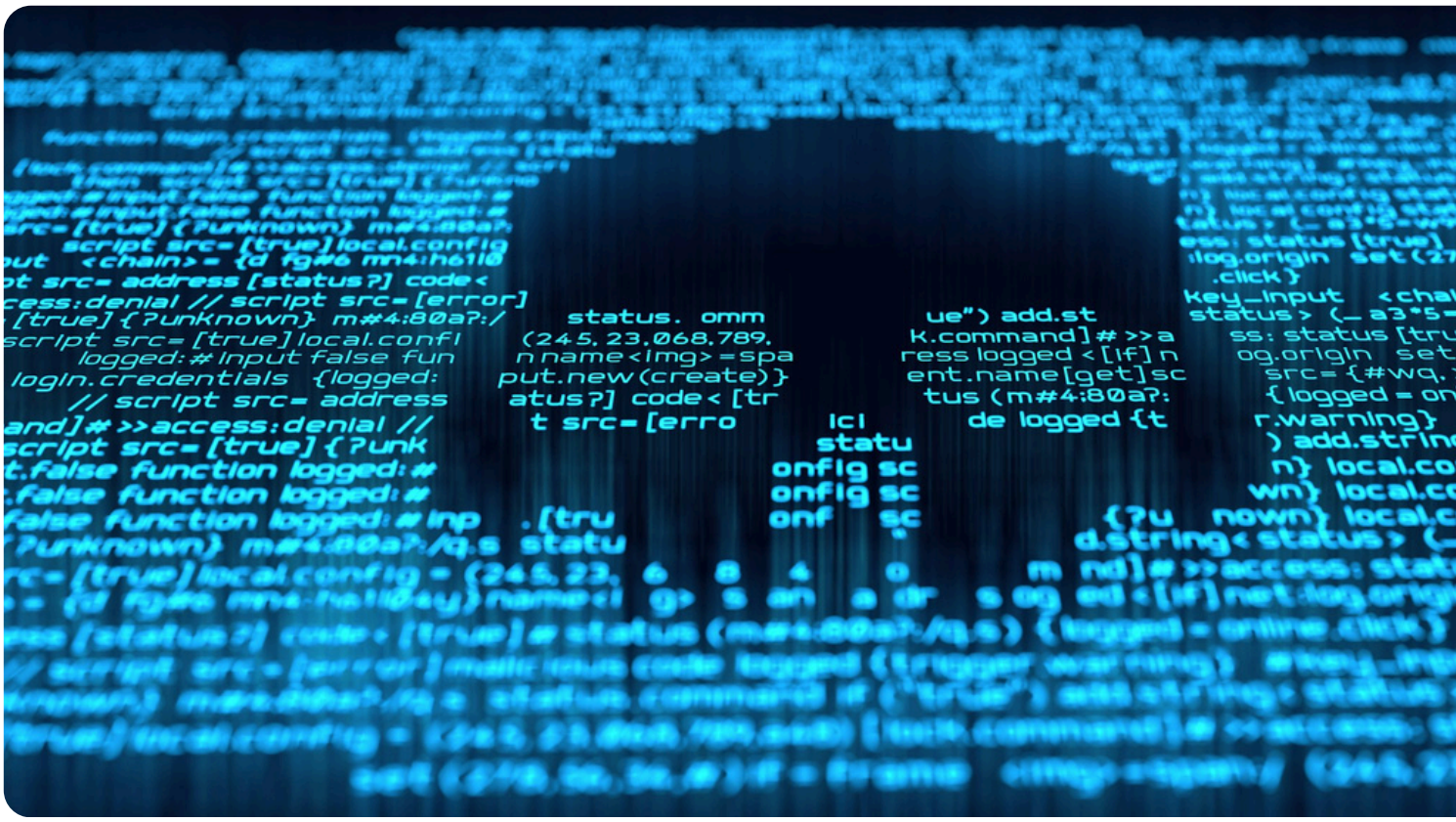
The good news is that reducing these risks doesn't require complicated technology. Simple steps can make a big difference.

Multi-factor authentication adds a second layer of protection when someone logs in.

Regular reminders to staff about suspicious emails help people recognise warning signs.

Clear processes for removing someone's access when they leave the practice prevent a very common security problem.

And keeping software up to date closes many of the doors attackers rely on.



Your data is more valuable **than you think**

If you ask most practice owners what client data they hold, the answer is usually something like names, phone numbers, and email addresses.

It's much more than that.

A typical practice management system may hold:

- Home addresses
- Payment card details
- Direct debit agreements
- Pet insurance policy numbers
- Microchip records
- Clinical histories
- Financial agreements with clients

For practices that work with agricultural clients, the system may also include information about property and livestock.

Patient records themselves can also have value. They can be used in insurance disputes, breeding records, and pedigree documentation.

When you start listing everything your system contains, it quickly becomes clear why criminals find it attractive.

Understanding what you hold also changes how you think about access.

Not everyone in the practice needs to see everything.

A receptionist rarely needs full access to clinical histories. A nurse doesn't normally need access to payment agreements.

Most modern practice management systems allow different levels of access for different roles.

That way, if someone's login details are ever compromised, the potential damage is limited.

Another important habit is removing access when staff leave.

Accounts that stay active after someone has left are an entirely avoidable security risk.

It's also worth remembering that data protection laws require practices to manage how long personal information is kept and when it should be deleted.

You should discuss this with whoever handles compliance for your practice.

When something **goes wrong**

Picture a Saturday morning when the practice is already busy.

Your practice management system suddenly won't load. Nobody can access appointment histories or patient records.

The phones are ringing, and a surgical patient is already prepped in theatre.

What happens next depends entirely on decisions made months earlier.

- Are your backups recent enough to be useful?
- Has anyone tested whether they can be restored?
- Is there a simple fallback plan written down somewhere?
- Does your team know where to find it?
- And if the system stays offline, do you have an IT support contact who treats that situation as an emergency?

Practices that recover quickly from these situations aren't always the ones with the most expensive systems. They're the ones that planned for failure in advance.

They have a short, written procedure, they've tested their backups, and they have someone they can call when things go wrong.

Often that preparation takes less than an hour. But it can make the difference between a short disruption and a day-long crisis.



Good technology gives you **time back**

When people talk about technology in vet practices, the conversation usually focuses on protection. Protecting data, systems, and the business.

But good technology gives you time back too.

And in a practice where clinical care is the priority, that time is incredibly valuable.

Think about the small frictions that build up across a typical week.

- Phone calls to book appointments that could be handled online overnight
- Reminder calls that someone must make manually
- Paper forms filled in at reception that later must be typed into the system
- End-of-day payment reconciliation done by hand
- Post-visit care instructions printed out and handed across the desk



None of these tasks are huge on their own, but across a whole team, they quickly add up.

A few hours a week can easily become several days of lost time across a year.

Modern systems can remove much of that friction.

- Automated appointment reminders reduce missed appointments
- Online booking handles routine scheduling without involving reception
- Digital forms feed directly into the practice management system
- Integrated payments reconcile automatically
- Post-visit instructions can be sent electronically

The clinical work that defines your practice doesn't change. What changes is how much time your team has to focus on it.

A quick technology self-check **for your practice**

If you're unsure how your practice compares, try answering a few simple questions. You don't need perfect answers. The goal is to spot potential gaps.

- [ ] ***Do you know exactly where your practice data is stored?***
- [ ] ***Has your backup been tested in the last year to confirm it can be restored?***
- [ ] ***If your practice management system went offline tomorrow morning, would your team know what to do?***
- [ ] ***Are staff accounts removed from all systems on the day someone leaves the practice?***
- [ ] ***Are all computers running supported, up-to-date software?***
- [ ] ***Do you know who to call if systems stop working on a Saturday morning?***

If you answered "I'm not sure" to any of these questions, that's ok. Many practices discover a few grey areas when they take a step back and review their systems properly.

The important thing is identifying them before they become problems.

What to look for in an **IT support partner**

Not every IT support provider understands the veterinary world.

Some have never stepped inside a clinic.

They may not know the main practice management systems used in the profession, like IDEXX or EzyVet.

They may not realise that imaging files from X-ray or ultrasound machines are far larger than normal business files and need specialised backup arrangements.

And they may not understand that a system failure on a Sunday morning is very different from one on a quiet weekday afternoon.

A good IT support partner takes the time to understand your environment. That shows up in practical ways.

They understand how your systems connect. Their support hours reflect the realities of your practice schedule. And they treat urgent problems with the urgency they deserve.

One easy way to test this is simply to ask questions.

Ask what experience they have with veterinary software.

Ask whether they've supported clinical environments before.

And ask how they handle emergencies outside normal office hours.

The answers usually tell you a lot.



What a simple technology review **looks like**

If a practice asks for a technology review, the process is usually straightforward. **It typically focuses on a few key areas:**

- ***Where practice data is stored and how it's backed up***
- ***Whether computers and software are properly supported and updated***
- ***Who currently has access to different systems***
- ***How secure remote access and staff devices are***
- ***And what would happen if a key system suddenly stopped working***

In many cases, the result is a handful of practical improvements that reduce risk and make day-to-day work easier.

Sometimes the review simply confirms that everything is already in good shape, which can be reassuring.

Getting the **foundations right**

Most vet practice owners chose the profession because they care about animals. Managing technology wasn't part of the plan.

The good news is that it doesn't need to take much time or attention.

Practices that handle technology well tend to run more smoothly.

They lose fewer clients to avoidable problems. And when something goes wrong, they recover faster.

They aren't necessarily the practices that spent the most on their systems.

Instead, they're the ones that made a series of sensible decisions about backups, security, access to data and what happens when something breaks.

Getting there is a series of small decisions, most of which take far less time than you might think.

If you'd like a second opinion on your practice's technology setup, we'd be happy to help.

We can review your current systems, explain anything that might need attention, and suggest practical improvements if they're needed.

Get in touch.

Acuit

CALL: 0141 255 1617
EMAIL: hello@acu-it.co.uk
WEBSITE: www.acu-it.co.uk

SCAN ME