Software

Your Microsoft 365 **health check**



When did you last look at your Microsoft 365 setup, rather than just using it?

A lot of business owners would say,**“not since it was set up”.** There’s nothing wrong with that; you have a business to run, and once email is working and everyone can get into their files, there’s no obvious reason to go poking around in the settings.

But in all businesses, things can quickly change. Someone joins the business and someone else leaves. A project kicks off, a Team gets created for it, and long after everyone’s moved on, that Team is still sitting there, unused. Somebody runs into a snag, changes a setting to get past it, and never thinks about it again.

It’s the ordinary, everyday stuff that comes with running a business.

All of this happens underneath a system that still looks and feels the same from where you’re sitting. Email arrives. Teams opens. Files are there when you go looking for them. So there’s not usually anything that prompts a closer look.

But what’s happening underneath could be costing money or leaving a door open that really shouldn’t be.

Better to find that out from a quick check than from a mistake...



1

Start with **your licenses**

Licensing is one of the easiest places for cost to build up, simply because it's tied to people rather than to anything you'd think to check.

When someone joins your business, a license gets added for them without much thought. When someone leaves, their account is usually disabled quickly, but the license attached to that account isn't always removed at the same time.

Say someone left the business a few months ago. Their access was switched off that week, but if the license was never cancelled, you've been paying for it every month since, for an account nobody's used.

While one license isn't a huge cost, add that up across a business that's had a few people come and go, and it adds up faster than you might expect.

Going through your current list of active licenses and checking each one against someone who still works for you is a straightforward way to find money that's being spent for no reason.

While you're doing that, look at whether people have the right type of license for what they do. Microsoft 365 comes in different tiers, and some include more than others.

A member of your finance team might need the full range of features, but someone who mainly sends email and stores a few files probably doesn't.

Paying for the top tier across your whole business, when only a handful of people use everything included in it, is a common and easy mistake to make.

2

Look at who **still has access**

This follows on naturally from licensing, but access deserves its own look, because more than what you're paying for, it's about what people can see and what they can do.

When someone leaves, switching off their account usually stops them logging in. But it doesn't always remove everything that account was connected to. Shared mailboxes, distribution lists, and permissions on specific folders can all be left behind, particularly if they were set up individually for that person.

The same happens with people who are still with you. Say someone was given access to a client folder for a project earlier in the year. The project finished a while ago, but nobody thought to remove the access once it was no longer needed, so it's still sitting there.

On its own, that's a minor loose end. Across a full business and everyone in it, those loose ends can add up to a lot of access that no longer needs to exist.



A useful way to check this is to focus on the most important areas. Look at who can currently access your financial records, your HR documents, and anything containing customer data. If that list includes anyone who's left the business, or anyone who's moved into a role where they no longer need that access, correct it sooner rather than later.

3

Clean up **Teams and SharePoint**

Clutter usually builds up in Teams and SharePoint fastest.

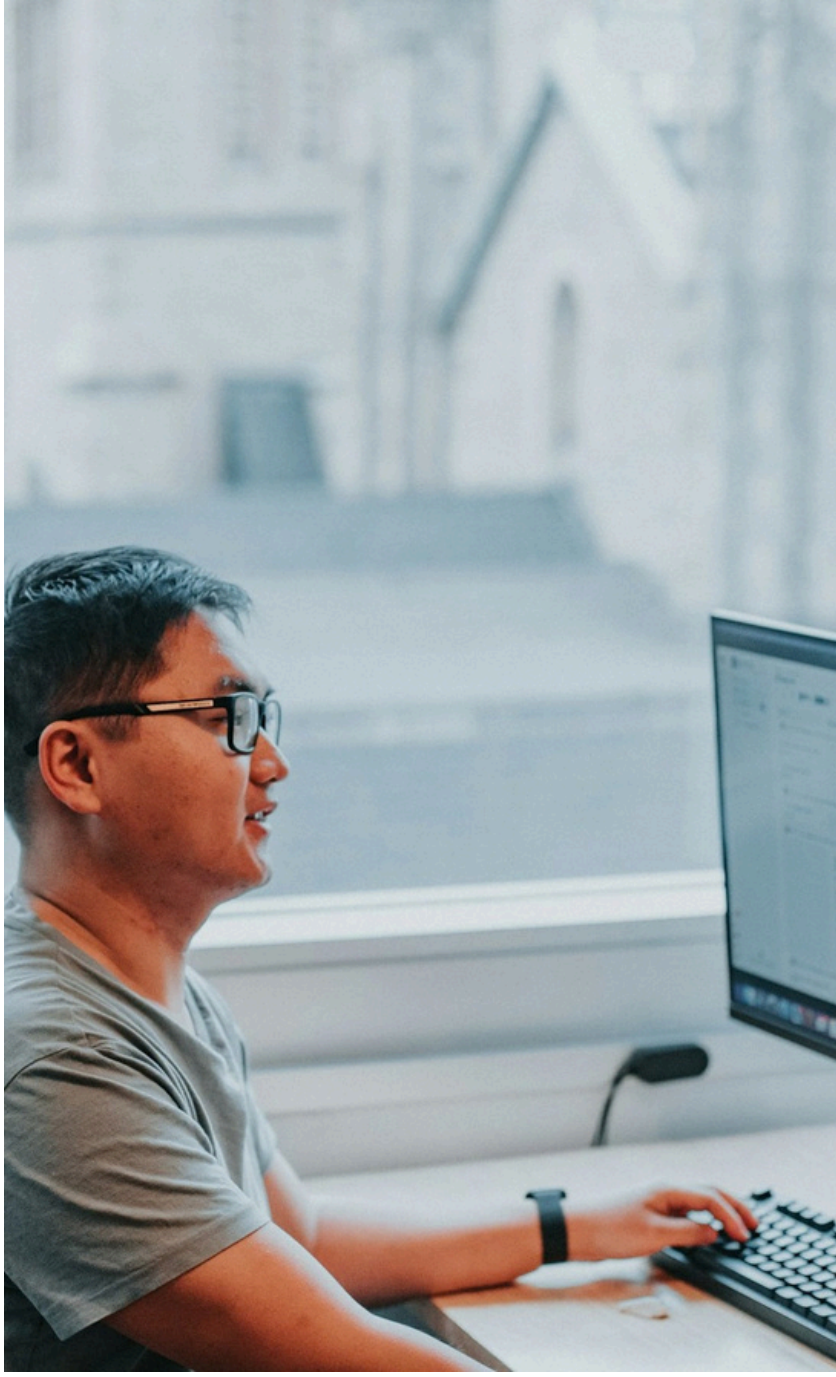
A new Team gets created for a client, a project, or an internal initiative. People are added, files are shared, and conversations happen in the channel. But once the work's finished, the Team isn't deleted. It stays sitting in your list of Teams long after anyone last opened it.

Across a year of projects and clients, that can leave you with dozens of Teams that nobody uses. Finding the one you need gets harder, because it's mixed in among a long list of others that stopped being relevant a while ago.

New employees joining the business face the same problem, without the benefit of knowing which ones aren't used anymore.

SharePoint develops a similar issue, but with documents rather than whole Teams.

A file is uploaded and shared, then a newer version is created somewhere else, and the original is never removed. That can leave you with several versions of the same document scattered across different locations, and no reliable way to know which one is current.



Going through your Teams and SharePoint sites and archiving or removing what's no longer needed makes the whole environment easier to work in. It also makes life considerably easier for anyone new who joins the business and needs to find their way around.

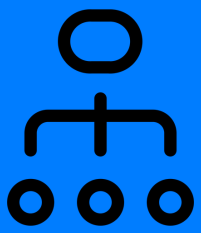
4

Check your ***automated processes***

If your business uses Power Automate, or any of the automated workflows built into Microsoft 365, these are worth a look too, because they're easy to forget once they're running.

A flow is created to solve a specific problem. Maybe it automatically saves email attachments to a particular folder or notifies a team when a form is submitted. It's set up, it works, and it's forgotten about, right up until the person who built it leaves the business or changes role.

If that flow was tied to their personal account rather than a shared one, it can stop working the moment their account is disabled. And nobody finds out until something that used to happen automatically… doesn't.



Going through your active flows, checking who owns each one, and deciding whether it's still needed is a small task that prevents an awkward surprise further down the line.

5

Check your ***security settings***

Security settings deserve a proper review on a regular basis, not just when something goes wrong.

Multi-factor authentication is the first thing to check. If it isn't switched on for every account in your business, that's a priority to fix before anything else on this list.

Some employees see it as a small inconvenience; an extra step when signing in. But from a security standpoint it remains one of the most effective ways to stop an account being accessed by someone who shouldn't have it.

File sharing settings need your attention too.

Microsoft 365 makes it easy to share a document with someone outside your business, which is useful day to day, but default settings on some accounts let files be shared more widely. A document meant for one supplier can end up accessible to anyone with the link, without anyone in the business realising.



Mailbox rules are another area to check while you're in there.

Most are harmless, created by an employee to sort or file certain emails automatically. Occasionally, though, a rule is created by someone who's gained access to an account without permission, forwarding emails to an address outside the business so they can be read without anyone noticing.

A periodic check across your mailboxes takes very little time and can catch something serious.



6

Review your **backups**

Microsoft 365 keeps your data available day to day, but availability and backup aren't the same thing.

Deleted emails, files, and Teams messages can usually be recovered, but only for a limited window. And that window is relatively short. If a file's deleted and nobody notices for a few months, or if something like a ransomware attack affects your data, the recovery options built into Microsoft 365 may not stretch far enough to help.

A proper backup keeps a separate copy of your data, so it can be restored regardless of what's happened within your Microsoft 365 environment. If your business doesn't currently have this in place, or if nobody's checked in a while that backups are running and can be restored, now is a good time to investigate.

7

Make space ***for what's coming***

Reviewing your Microsoft 365 setup isn't only about tidying up what's already happened. It also puts you in a stronger position for whatever comes next.

More businesses are looking at tools like Copilot and other AI features built into the platform. Those tools work best in an environment where information is well organised, access is properly managed, and security is solid. A health check now means you're approaching new technology from a stronger starting point, rather than trying to layer it on top of a system that's still carrying months of unfinished tidying up.



Even setting AI aside, a business running on a clean, well-managed Microsoft 365 environment is easier to work in day to day. Files are easier to find, there's less to explain to new starters, and there's less risk of something important being missed because it was buried.

Where *to start*

None of this needs to happen in one sitting, and none of it needs to be complicated. A short review covering the following will catch most of the things that can build up in Microsoft 365:

- **Licenses:** Are you paying for anyone who's no longer with the business, or on a higher tier than they need?
- **Access:** Can anyone see files, folders, or systems they no longer need?
- **Teams and SharePoint:** Are there old Teams, sites, or duplicate documents worth clearing out?
- **Automated flows:** Is anything running that's tied to someone who's left or changed roles?
- **Security settings:** Is multi-factor authentication switched on everywhere, and are file sharing and mailbox rules set up sensibly?
- **Backups:** Are they running, and have they been tested?

Of course, finding time for all of this alongside everything else you've got going on isn't always easy. If you'd like help going through it, we're happy to take a look and talk you through what we find.

Get in touch.

CALL: 01727 326666
EMAIL: hello@jedi-services.com
WEBSITE: www.jedi-services.com