BITWISE-IT BUSINESS TOOLKIT

Backing Up Your Business Documents

A practical guide for Windows and Mac

Bitwise-IT Limited

Wickford, Essex · 01268 218301

info@bitwise-it.co.uk · bitwise-it.co.uk

Before you begin

> This guide shows you how to set up a second copy of the documents your business could not operate without — the ones that would stop you trading if they vanished this afternoon. It takes about twenty minutes to set up and five minutes a week to keep current.

Two things to get straight first

The drive this came on is not your backup. It is a toolkit — guides, checklists and planners. Promotional USB sticks are small, and cheap flash memory living in a coat pocket is the last thing anyone should trust with their only copy of the accounts. Keep this drive for the documents; buy a proper external drive for the backup. A decent 1TB portable drive costs less than a working lunch and will hold everything discussed here many times over.

There is no software on this drive, deliberately. We are a cyber security business, and the first rule we teach is not to run programs from a USB stick somebody handed you. We are not about to break our own rule to save you a download. Everything you need is linked from our toolkit page, straight from the people who make it, at the current version.

Current recommended backup tools and setup notes

bitwise-it.co.uk/toolkit

Updated as versions change — so this guide does not go stale

What a real backup looks like

The widely used benchmark is the **3-2-1 rule**: three copies of your data, on two different types of media, with at least one copy kept somewhere else. An external drive gets you a solid second copy. It is unaffected by an internet outage, costs nothing to run, and is entirely under your control — but it is only as recent as the last time you ran it, and it burns in the same fire as the laptop.

Copy	Where it lives	Protects against
1. Working copy	Your PC or Mac, and Microsoft 365	Nothing — this is the thing at risk
2. Local backup	An external drive you own, kept away from the computer	Deleted files, failed disks, dropped laptops
3. Off-site backup	A managed cloud backup, including your Microsoft 365 data	Fire, flood, theft, ransomware, human error

This guide covers copy number two. Copy number three is where most small businesses have a gap they do not know about, and it is the one we most often get called about after something has gone wrong.

Step 1 — Decide what to back up

> Most businesses lose time backing up the wrong things. The aim is not to copy everything; it is to copy what you cannot rebuild or re-obtain.

Start with these

Category	Typical documents
Finance	Invoices raised and received, bank statements, VAT records, payroll files, year-end accounts, expense receipts
Legal & company	Contracts, terms of business, insurance certificates, leases, certificate of incorporation, licences and registrations
Clients	Client files and correspondence, quotes and proposals, project records, signed agreements, deliverables
People	Employment contracts, right-to-work evidence, appraisals, training records, HR policies
Operations	Templates and letterheads, price lists, supplier details, standard operating procedures, asset and warranty records
Identity	Logos, brand assets, website content and photography you own

You can usually skip these

- **Software installers and downloads** — re-downloadable, and they eat your drive space.
- **Email exported to PST files** — back email up properly at tenant level instead. PSTs age badly and corrupt quietly.
- **System and program folders** — these will not restore usefully onto a different machine.
- **Anything in SharePoint or OneDrive that has not been made available offline** — see the warning below, because this one catches almost everybody.

> **THE PLACEHOLDER TRAP — READ THIS ONE TWICE**
>
> OneDrive on Windows (Files On-Demand) and iCloud Drive on Mac (Optimise Mac Storage) save space by keeping files in the cloud and leaving a small placeholder on your machine. A backup tool copying those folders may copy the placeholders and not your actual documents — giving you a backup that looks complete and contains nothing.
>
> **Windows:** right-click the folder in File Explorer → **Always keep on this device**. Wait for the solid green circle with a white tick before backing up. **Mac:** System Settings → Apple Account → iCloud → iCloud Drive, and turn off **Optimise Mac Storage**, or right-click the folder and choose **Download Now**.

> **A WORD ABOUT MICROSOFT 365**
>
> If your business runs on Microsoft 365, be clear about what Microsoft actually covers. They guarantee the platform stays up; the contents of your mailboxes, SharePoint sites and Teams conversations remain your responsibility, and the default retention windows are shorter than most people assume. A local backup of your documents does not cover any of it. This is the single most common gap we find.

Write your list down

Before you touch any software, note the folders you want copied. Three or four well-chosen folders beat twenty vague ones, and the list makes everything that follows much quicker.

Step 2 — Choose your tool

You do not need to spend money on backup software, but you do need to choose carefully — and there is a licensing trap in this category that catches a great many small businesses.

"FREE" OFTEN MEANS "FREE FOR HOME USE"

Several of the best-known free backup and sync tools are licensed for private use only. Using them in a business — including a one-person limited company — requires a paid licence, and plenty of firms are technically in breach without ever realising it. Before you install anything, find the licence page and check that commercial use is permitted. If a tool is genuinely open source under a permissive licence, it will say so plainly.

Our toolkit page lists current tools that are free for business use, so you do not have to work this out yourself.

What to look for

Whichever tool you settle on, these are the features that separate a backup you can rely on from one that merely runs:

- ☐ **It shows you what it will do before it does it.** A preview of what is about to be copied, changed or deleted — and a chance to stop.
- ☐ **It only copies what has changed.** Your first run may take an hour; every run after it should take seconds. If it copies everything every time, you will stop doing it.
- ☐ **It keeps deleted and overwritten files for a while.** Often called versioning. This is what saves you when the problem is not a dead disk but a mistake made three days ago.
- ☐ **It can save the job and re-run it.** If you have to set it up from scratch each week, you will not do it each week.
- ☐ **It handles the drive letter changing.** Windows gives external drives whatever letter is free, so a saved job pointed at `E:` can fail when the drive turns up as `G:`. Good tools can find the drive by its name instead.
- ☐ **It tells you clearly when something failed.** Silent failure is the defining characteristic of a backup that lets you down.

Plain files or a backup archive?

Tools fall into two camps, and the difference matters more than the feature lists suggest.

Approach	How the backup looks on the drive	The trade-off
Plain file copy	An ordinary folder structure. You can plug the drive into any computer and open a document directly.	Simplest to restore from in a crisis. You must encrypt the drive yourself.
Backup archive	Compressed, encrypted blocks. You need the backup software installed to get anything back out.	Encryption and space saving are built in, but restoring means installing software first.

For a small business, plain file copy is usually the kinder choice. The worst day to discover you need to install and configure software before you can open an invoice is the day the server died.

Current recommendations, licence notes and download links

bitwise-it.co.uk/toolkit

Always download software from the vendor, never from a USB drive you were given

Step 3 — Encrypt the drive first

> Do this before you copy a single file. It takes two minutes and it is the difference between a lost drive being an annoyance and a lost drive being a reportable data breach.

Business documents almost always contain personal data — staff details, client contacts, invoices with names on them — which brings them within scope of UK GDPR. An unencrypted drive left on a train is a notifiable incident. An encrypted one generally is not.

1. **Windows 10 or 11 Pro**
   Right-click the drive in File Explorer → **Turn on BitLocker** → choose a password → save the recovery key somewhere safe. Not on the drive itself, and not in a document called "passwords".

2. **Mac**
   In Finder, right-click the drive → **Encrypt** → set a password and a hint. The drive must be formatted as APFS or Mac OS Extended for this option to appear; if it is not, you will need to erase and reformat it first.

3. **Windows Home**
   BitLocker is not included. Either use a backup tool that encrypts its own archive, or buy a hardware-encrypted drive with a keypad. Do not simply skip this step.

> **STORE THE RECOVERY KEY PROPERLY**
> A password manager is the right home for it. If the encryption password is lost and the recovery key with it, the data is gone — that is the entire point of encryption, and no amount of technical skill will get it back.

Step 4 — Set up the job

The exact buttons vary by tool, but every one of them asks you the same three questions.

1. **What am I copying? (the source)**
   The folders from your list. Most tools let you add several in one job, so Documents, Desktop and a shared work folder can all be covered by a single run.

2. **Where am I copying it to? (the destination)**
   A folder on your external drive, such as `Business Backup`. Where the tool offers it, refer to the drive by name rather than by letter so the job survives Windows reassigning it.

3. **What happens to changes and deletions? (the mode)**
   See the table below. For a business backup you want a mirror *with* versioning: the drive matches your documents, but anything deleted or overwritten is kept for a while first.

Mode	What it does	Use it when
Mirror	Makes the drive an exact copy. Files you delete on the computer are deleted from the drive too.	You want a faithful snapshot and accept that deletions carry across
Mirror with versioning	As above, but anything deleted or overwritten is moved into a dated folder first.	**Recommended.** A clean copy plus a safety net against mistakes
Update / additive	Copies new and changed files but never deletes anything from the drive.	You want an accumulating archive and have space to spare
Two-way sync	Changes on either side are copied to the other.	Rarely right for backup. Avoid unless you have been advised otherwise

Run the job, then **read the screen before you confirm**. On the first run it will want to copy everything, which is normal. On later runs, if it proposes deleting hundreds of files you did not delete, stop — that pattern is a classic ransomware symptom, and the section on page 6 explains what to do.

Step 5 — Check it actually worked

> A backup nobody has tested is an assumption, not a backup. Spend five minutes on this now and repeat it once a quarter.

- [ ] **Read the summary.** Every decent tool reports what it copied and whether anything failed. Zero errors is the target; "a few errors" is a habit that ends badly.
- [ ] **Browse the drive.** Open a few folders. Do the file sizes look right, or are they suspiciously tiny? Tiny means cloud placeholders — go back to page 2.
- [ ] **Open a real document from the drive.** A recent invoice or contract. Confirm it is genuinely the current version and not one from six months ago.
- [ ] **Do a restore test.** Copy a file from the drive back to your Desktop and open it. That is a real restore, and it is the only proof that counts.

> **EJECTING SAFELY**
>
> **Windows:** the USB icon in the system tray → Eject. **Mac:** the eject arrow in Finder, or drag the drive to the Bin. Pulling the drive out mid-write is one of the most common causes of a corrupted backup, and you will not find out until you need it.

Your routine

The whole point of saving the job is that the ongoing effort is trivial. Put it in the calendar and it will happen.

How often	What to do
Weekly	Plug in the drive, unlock it, run the saved job, check the summary shows no errors, eject, and put the drive away somewhere other than beside the computer.
Monthly	Open one document directly from the drive to confirm the backup is current and readable.
Quarterly	Full restore test. Copy a folder back and open several files. Review whether your list of folders is still the right list — businesses move their data around more than they realise.
Every two to three years	Replace the drive. All storage wears out, and a drive that has been rattling around for years owes you nothing.

Where to keep it

Not plugged into the computer. A backup that lives permanently in the USB port is encrypted along with everything else when ransomware arrives, and stolen along with the laptop when the office is broken into. A locked drawer is better; another building is better still. And because the drive is encrypted, keep the recovery key somewhere different again.

Restoring files

1. **One or two files**

   Plug in the drive, unlock it, find the file and copy it back. If you chose a plain file copy tool, no software is needed at all.

2. **A whole folder**

   Set up a job the other way round — drive as source, your computer as destination — and use an additive mode rather than mirror, so nothing on the computer gets deleted. Preview carefully before confirming.

3. **A version you deleted earlier**

   Look in the versioning folder on the drive. Previous copies are filed there under the date they were replaced or removed.

> **IF YOU THINK YOU HAVE BEEN HIT BY RANSOMWARE**
>
> **Do not plug this drive in.** Connecting a backup to an infected machine is the single most common way businesses lose their last clean copy. Disconnect the affected computer from the network but leave it switched on, and get help immediately.
>
> Report it: **0300 123 2040** reaches Action Fraud (now Report Fraud), who staff a line around the clock for organisations under live attack. If personal data may have been exposed you may also need to notify the ICO within 72 hours. Our separate ransomware guide on this drive walks through the first hour in detail.

Troubleshooting

What you see	What to do
The drive has a different letter and the saved job fails	Edit the job to refer to the drive by its name rather than its letter, if your tool supports it. Otherwise repoint the job.
Files copy but are only a few kilobytes	You are copying cloud placeholders. Make the folders available offline first — see page 2 — then run again.
Files are skipped on a Mac, or permission errors appear	macOS blocks apps from reading Documents, Desktop and Downloads until you allow it. System Settings → Privacy & Security → Full Disk Access → enable your backup tool, then restart it.
The drive fills up	Usually the versioning folder has grown. Delete the oldest dated folders, shorten how long versions are kept, or narrow what you are backing up.
"The disk is write-protected"	Check for a physical switch on the drive, and confirm you unlocked the encryption with your password rather than dismissing the prompt.
The job wants to delete a large number of files you did not delete	Stop. Do not continue. This is what ransomware looks like from a backup tool's point of view.
Files with very long names or deep folders fail	Usually a path-length limit. Shorten the folder structure, or ask us about enabling long path support.

Where a local backup stops being enough

> Everything in this guide protects you against the everyday disasters. It does not protect you against the ones that close businesses.

- **It is only as recent as the last run.** A backup taken on Friday does not help with a Thursday disaster the following week.
- **It is on-site.** Fire, flood and theft take the original and the copy together.
- **Microsoft 365 is not covered.** Your email, SharePoint and Teams content is your responsibility, and most businesses find this out at the worst possible moment.
- **Nobody is checking it.** Manual backups fail quietly. The moment you discover the failure is the moment you needed the backup.
- **It depends on one person remembering.** When that person is on holiday, or has left, the routine stops.

None of that means a local backup is not worth doing — it absolutely is, and if this guide gets you as far as a working weekly routine you are ahead of most small businesses. But it should be the second layer, not the only one.

We are happy to look at this with you

Bitwise-IT is an Essex-based IT partner working with businesses from around five users upwards. Every package we run includes managed Microsoft 365 backup, proactive monitoring and patching, and a helpdesk that answers — with enhanced protection available as your risk profile grows.

If you would like an honest opinion on where your gaps are, we will review your setup and tell you straight. No pressure, no jargon, and no obligation to buy anything.

01268 218301 · info@bitwise-it.co.uk · bitwise-it.co.uk