Blog Entries

Draft Blogs for Website to Review.

After written up, please tag technical/reviews in to the blog

Once Review is completed, please can reviewee's comment on the blog to say completed/ changes made.

- How Small Businesses Can Improve Cybersecurity Without a Huge Budget
- Signs Your Business Has Outgrown Its Current IT Setup
- Sustainable Cloud Migration: A Better Fit for Businesses Looking Ahead
- Is Your Business Ready VoIP Ready for the Big Copper Switch off?
- Don't Lose Everything: A Beginner's Guide to Backing Up Your Mac
- Don't Lose Everything: A Beginner's Guide to Backing Up Your Windows PC
- Nextcloud Explained: The Smart, Private Alternative to Dropbox and Google Drive
- Our Recommended Password Managers (And Why You Should Be Using One)
- IT Equipment Recycling UK: Why Your Old Tech Doesn't Just Disappear

How Small Businesses Can Improve Cybersecurity Without a Huge Budget

/small-business-cybersecurity-uk-budget

Signs Your Business Has Outgrown Its Current IT Setup

Sustainable Cloud Migration: A Better Fit for Businesses Looking Ahead

Is Your Business Ready VoIP Ready for the Big Copper Switch off?

Don't Lose Everything: A Beginner's Guide to Backing Up Your Mac

Picture this: you spill your morning coffee on your MacBook, or it gets stolen at a coffee shop, or it just decides — after years of loyal service — that today is the day it stops working. Everything gone. Your photos, your documents, your work files. All of it.

It's a nightmare scenario, but here's the thing: it's almost entirely avoidable. Backing up your Mac takes surprisingly little effort once you know how, and the peace of mind it gives you is genuinely priceless. Let's walk through exactly what to do.

Why Backing Up Your Mac Actually Matters

Most of us don't think about backups until something goes wrong — and by then, it's too late. Here are the real reasons you should make this a habit:

Hardware fails without warning. Even the best MacBooks have a lifespan, and hard drives can die unexpectedly. When they do, there's often no second chance to retrieve your files.

Accidents happen. Drops, spills, and theft are more common than you'd think. Repairs can sometimes recover data, but it's expensive and not guaranteed.

Ransomware and malware are real threats. Malicious software can encrypt or delete your files. A recent, clean backup means you can simply restore your system and carry on.

macOS upgrades can occasionally go wrong. Most of the time, updating macOS is smooth — but not always. Having a backup before a major update is just good practice.

The bottom line: your data is worth protecting, and backups are the cheapest insurance policy you'll ever take out.

The 3-2-1 Backup Strategy: A Simple Rule to Live By

Security and IT professionals swear by a principle called the **3-2-1 strategy**. It sounds technical, but it's actually very easy to understand:

- **3** copies of your data (the original + 2 backups)
- **2** different storage types (e.g., an external hard drive and a cloud service)
- **1** copy stored offsite (e.g., cloud storage or a drive kept at a different location)

Why does this matter? Because a single backup can fail too. If your Mac and your external hard drive are sitting next to each other and there's a fire or a flood, both are gone at once. The 3-2-1 rule makes sure you're covered against multiple failure scenarios at the same time.

For most Mac users, this looks like: **Time Machine on an external drive** + **Nextcloud for offsite cloud storage**. That covers all three bases without much extra effort.

How to Back Up Your Mac: Step by Step

Option 1: Time Machine (Built-In and Easy)

Time Machine is Apple's built-in backup tool, and it's brilliant for beginners. It runs automatically in the background and saves hourly, daily, and weekly snapshots of your files.

What you'll need: An external hard drive or SSD (aim for at least twice the storage capacity of your Mac).

1. Plug your external drive into your Mac.
2. Open **System Settings** (or System Preferences on older macOS versions).
3. Click **General**, then **Time Machine**.
4. Click **Add Backup Disk** and select your external drive.
5. Turn on **Back Up Automatically**.

That's it. Time Machine will now back up your Mac regularly without you having to think about it. You can also use it to restore individual files, or your entire Mac, if things go wrong.

> **Tip:** Keep your external drive plugged in as often as possible — ideally whenever you're at your desk — so Time Machine can do its job regularly.

Option 2: Nextcloud (Your Offsite Copy)

Nextcloud is a private, self-hosted cloud storage platform — and it's the solution we use and recommend here at Tranquil IT. Rather than storing your files on Apple's or Google's servers, Nextcloud keeps your data on infrastructure you or your IT provider controls, while still giving you all the convenience of cloud sync and access from any device.

Once set up, the Nextcloud desktop app syncs your chosen folders automatically in the background — just like iCloud or Dropbox — and you can access everything from any browser or your phone. It satisfies the "offsite" part of the 3-2-1 rule perfectly, while keeping your data genuinely private and secure.

We handle the hosting and setup for you, so there's nothing technical to worry about. Read our full guide to Nextcloud to find out why we think it's the best cloud option for most users, or get in touch and we'll walk you through it.

Putting It All Together: Your 3-2-1 Setup

Here's a simple setup that ticks all three boxes:

Copy	Method	Location
Original	Your Mac	At home / on you
Backup 1	Time Machine on external drive	At home
Backup 2	Nextcloud	Cloud (offsite)

With this in place, you're protected against hardware failure, accidental deletion, theft, and even natural disasters.

A Few Extra Tips to Keep Your Backups Healthy

- **Test your backups occasionally.** Open Time Machine and try restoring a random file to make sure it works. A backup you've never tested is a backup you can't fully trust.
- **Label your drives.** If you have multiple external drives, label them clearly so you always know which is your backup drive.
- **Set a reminder.** If you're not using automatic backups, set a monthly calendar reminder to do it manually.
- **Don't ignore low-storage warnings.** If your backup drive is nearly full, your backups will stop working properly.

Start Today — It Only Takes 10 Minutes

If you've been putting off setting up backups, today is a great day to start. All you need is an external drive and 10 minutes to get Time Machine running. Add Nextcloud on top, and you've instantly got a solid 3-2-1 setup that will protect you from the unexpected.

Your future self will thank you.

Have questions about setting up your Mac backup, or not sure which external drive to buy? Get in touch with the Tranquil IT team — we're happy to help. Email us at support@tranquilit.net or give us a call on 01279 658331.

About This Post

SEO Recommendations:

- **Primary keyword:** "how to back up your Mac" — used in headline and first section
- **Related keywords to use:** "Mac backup", "Time Machine backup", "Nextcloud backup Mac", "3-2-1 backup strategy", "private cloud storage Mac"
- **Meta description (under 160 chars):** "Learn how to back up your Mac in minutes using Time Machine and Nextcloud — plus the 3-2-1 strategy that keeps your files safe no

matter what."

- **Internal linking opportunity:** Link to the Nextcloud guide, the Windows backup guide, and any Tranquil IT service pages
- **External linking opportunity:** Apple's official Time Machine support page, Nextcloud's official website
- **Image alt text suggestion:** "MacBook connected to external hard drive for Time Machine backup"

Suggested URL Slug - /blog/how-to-back-up-your-mac

Don't Lose Everything: A Beginner's Guide to Backing Up Your Windows PC

Picture this: your laptop takes a tumble off the desk, or a ransomware attack locks you out of all your files, or Windows decides — at the worst possible moment — to stop working entirely. Everything gone. Your photos, your documents, your work files. All of it.

It's a nightmare scenario, but here's the thing: it's almost entirely avoidable. Backing up your Windows PC takes surprisingly little effort once you know how, and the peace of mind it gives you is genuinely priceless. Let's walk through exactly what to do.

Why Backing Up Your Windows PC Actually Matters

Most of us don't think about backups until something goes wrong — and by then, it's too late. Here are the real reasons you should make this a habit:

Hardware fails without warning. Even a well-looked-after PC has a lifespan, and hard drives can die unexpectedly. When they do, there's often no second chance to retrieve your files.

Accidents happen. Drops, spills, and theft are more common than you'd think. Repairs can sometimes recover data, but it's expensive and not guaranteed.

Ransomware and malware are real threats. Windows is the most widely targeted operating system in the world, and malicious software can encrypt or delete your files in minutes. A recent, clean backup means you can simply restore your system and carry on.

Windows updates can occasionally go wrong. Most of the time, updating Windows is smooth — but not always. Having a backup before a major update is just good practice.

The bottom line: your data is worth protecting, and backups are the cheapest insurance policy you'll ever take out.

The 3-2-1 Backup Strategy: A Simple Rule to Live By

Security and IT professionals swear by a principle called the **3-2-1 strategy**. It sounds technical, but it's actually very easy to understand:

- **3** copies of your data (the original + 2 backups)
- **2** different storage types (e.g., an external hard drive and a cloud service)
- **1** copy stored offsite (e.g., cloud storage or a drive kept at a different location)

Why does this matter? Because a single backup can fail too. If your PC and your external hard drive are sitting next to each other and there's a fire or a flood, both are gone at once. The 3-2-1 rule makes sure you're covered against multiple failure scenarios at the same time.

For most Windows users, this looks like: **File History on an external drive** + **Nextcloud for offsite cloud storage**. That covers all three bases without much extra effort.

How to Back Up Your Windows PC: Step by Step

Option 1: File History (Built-In and Easy)

File History is Windows' built-in backup tool, and it's a great starting point for beginners. Once set up, it automatically saves copies of your files at regular intervals so you can restore them if something goes wrong.

What you'll need: An external hard drive or SSD (aim for at least twice the storage capacity of your PC).

1. Plug your external drive into your PC.
2. Open the **Start menu** and go to **Settings**.
3. Go to **System** > **Storage** > **Advanced storage settings** > **Backup options** (Windows 11), or search for **"Backup settings"** in the Start menu.
4. Under **Back up using File History**, click **Add a drive** and select your external drive.
5. Turn on **Automatically back up my files**.

That's it. File History will now back up your files regularly in the background. You can also use it to browse previous versions of your files and restore anything you've accidentally changed or deleted.

> **Tip:** Keep your external drive plugged in as often as possible — ideally whenever you're at your desk — so File History can do its job regularly.

Option 2: Nextcloud (Your Offsite Copy)

Nextcloud is a private, self-hosted cloud storage platform — and it's the solution we use and recommend here at Tranquil IT. Rather than storing your files on Microsoft's or Google's servers, Nextcloud keeps your data on infrastructure you or your IT provider controls, while still giving you all the convenience of cloud sync and access from any device.

Once set up, the Nextcloud desktop app syncs your chosen folders automatically in the background — just like OneDrive or Dropbox — and you can access everything from any browser or your phone. It satisfies the "offsite" part of the 3-2-1 rule perfectly, while giving you far greater privacy and control than any mainstream cloud service.

We handle the hosting and setup for you, so there's nothing technical to worry about. Read our full guide to Nextcloud to find out why we think it's the best cloud option for most users, or get in touch and we'll walk you through it.

Putting It All Together: Your 3-2-1 Setup

Here's a simple setup that ticks all three boxes:

Copy	Method	Location
Original	Your PC	At home / on you
Backup 1	File History on external drive	At home
Backup 2	Nextcloud	Cloud (offsite)

With this in place, you're protected against hardware failure, accidental deletion, theft, and even natural disasters.

A Few Extra Tips to Keep Your Backups Healthy

- **Test your backups occasionally.** Open File History and try restoring a random file to make sure it works. A backup you've never tested is a backup you can't fully trust.
- **Label your drives.** If you have multiple external drives, label them clearly so you always know which is your backup drive.
- **Set a reminder.** If you're not using automatic backups, set a monthly calendar reminder to do it manually.
- **Don't ignore low-storage warnings.** If your backup drive is nearly full, your backups will stop working properly.
- **Keep Windows updated.** Security patches help protect your files from malware in the first place — backups and updates work best together.

Start Today — It Only Takes 10 Minutes

If you've been putting off setting up backups, today is a great day to start. All you need is an external drive and 10 minutes to get File History running. Add Nextcloud on top, and you've instantly got a solid 3-2-1 setup that will protect you from the unexpected.

Your future self will thank you.

Have questions about setting up your Windows backup, or not sure which external drive to buy? Get in touch with the Tranquil IT team — we're happy to help. Email us at support@tranquilit.net or give us a call on 01279 658331.

About This Post

SEO Recommendations:

- **Primary keyword:** "how to back up your Windows PC" — used in headline and first section

- **Related keywords to use:** "Windows backup", "File History backup", "Nextcloud backup Windows", "3-2-1 backup strategy", "back up Windows 11", "private cloud storage Windows"
- **Meta description (under 160 chars):** "Learn how to back up your Windows PC in minutes using File History and Nextcloud — plus the 3-2-1 strategy that keeps your files safe no matter what."
- **Internal linking opportunity:** Link to the Nextcloud guide, the Mac backup guide, and any Tranquil IT service pages
- **External linking opportunity:** Microsoft's official File History support page, Nextcloud's official website
- **Image alt text suggestion:** "Windows laptop connected to external hard drive for File History backup"

Suggested URL Slug - /blog/how-to-back-up-your-windows-pc

Nextcloud Explained: The Smart, Private Alternative to Dropbox and Google Drive

You've probably used Dropbox, Google Drive, or OneDrive at some point. They're convenient — but they come with a trade-off most people don't think about: your files are sitting on someone else's servers, governed by their privacy policies, subject to their pricing changes, and accessible to them if they ever decide to look.

What if you could have all the convenience of cloud storage, but with full control over where your data actually lives? That's exactly what Nextcloud offers — and it's one of the reasons we at Tranquil IT use and recommend it to our customers.

So, What Is Nextcloud?

Nextcloud is an open-source file sharing and collaboration platform. Think of it as your own private version of Google Drive — you get file storage, syncing across devices, sharing with others, and much more, but the data is hosted on a server that *you* (or your IT provider) controls.

It's not a subscription service owned by a tech giant. It's software that runs on your own infrastructure, which means your files stay yours — full stop.

Nextcloud is used by everyone from individuals protecting their personal photos to large organisations managing sensitive business documents. It's trusted by governments, healthcare providers, and businesses across the world precisely because of the privacy and control it offers.

Why Nextcloud Stands Out

Your Data Stays Private

With services like Google Drive or Dropbox, your files are stored on their servers — in data centres you have no visibility into, under terms and conditions that can change at any time. Nextcloud flips this entirely. Your data is stored on infrastructure you control, and nobody else has access to it unless you choose to share it.

For businesses handling client data, sensitive documents, or anything subject to data protection regulations like GDPR, this isn't just a nice-to-have — it's essential.

It Works Just Like the Cloud Storage You Already Know

Nextcloud isn't some clunky, complicated alternative that requires a technical degree to use. It has apps for Windows, Mac, iPhone, and Android that sync your files automatically in the background — just like Dropbox or OneDrive. You can also access everything through a web browser from any device.

Sharing a file or folder with someone is as simple as generating a link, just like you would in Google Drive. You can set permissions, add passwords to shared links, and set expiry dates — giving you far more control than most mainstream services offer.

No Surprise Price Hikes or Storage Limits Dictated by Someone Else

With commercial cloud services, you're at the mercy of their pricing decisions. Storage plans get restructured, free tiers shrink, and prices go up. With Nextcloud, your storage capacity is defined by the hardware it runs on — and scaling up is straightforward.

For businesses in particular, this predictability makes budgeting much simpler.

It Goes Way Beyond File Storage

Nextcloud isn't just a place to park your files. It's a full collaboration platform. Out of the box (and through its extensive library of apps), it supports:

- **Nextcloud Talk** — secure video calls and messaging, without your conversations passing through a third-party server
- **Nextcloud Calendar and Contacts** — sync your calendar and address book across all your devices
- **Collaborative document editing** — work on documents together in real time, similar to Google Docs

- **Automatic photo backup** — your phone's photos can back up directly to your Nextcloud, just like iCloud or Google Photos
- **Task management** — keep track of to-dos without a separate app

It essentially replaces several different subscription services in one.

It's Built With Security in Mind

Nextcloud is developed by a large open-source community and a dedicated security team. Because the code is open source, it's continuously scrutinised by security researchers around the world — which actually makes it more transparent and trustworthy than closed, proprietary alternatives.

It supports end-to-end encryption, two-factor authentication, audit logging, and fine-grained access controls. For businesses, these aren't optional extras — they're built in.

How Nextcloud Fits Into the 3-2-1 Backup Strategy

If you've read our guides on backing up your Mac or Windows PC, you'll be familiar with the **3-2-1 backup rule** — keeping 3 copies of your data, on 2 different types of storage, with 1 copy stored offsite.

Nextcloud fits perfectly into this strategy as your offsite copy. Because it runs on a separate server (either on your premises in a different location, or hosted by a provider like Tranquil IT), your Nextcloud instance acts as an independent, always-available backup of your important files — separate from your local devices entirely.

Copy	Method	Location
Original	Your PC or Mac	At home / office
Backup 1	External hard drive (Time Machine / File History)	At home / office
Backup 2	Nextcloud	Offsite server or hosted infrastructure

Combined with automatic sync from your devices, Nextcloud means your files are protected and accessible — even if your local hardware fails completely.

Is Nextcloud Right for You?

Nextcloud is a great fit if you:

- Want full control and privacy over where your files are stored
- Are a business handling sensitive or regulated data
- Are tired of paying increasing subscription fees to multiple cloud services
- Want a single platform for file storage, sharing, communication, and collaboration
- Are looking to tick the "offsite backup" box in your data protection strategy

It does require a server to run on — which is where Tranquil IT comes in. We can host and manage a Nextcloud instance for you, handle all the setup and maintenance, and make sure it's properly secured and backed up. You get all the benefits of Nextcloud without needing to worry about the technical side.

Ready to Find Out More?

If you're interested in Nextcloud — whether for your home, your business, or just to understand whether it's the right fit — we'd love to have a conversation. Get in touch with the Tranquil IT team and we can walk you through your options.

Email us at support@tranquilit.net or give us a call on 01279 658331.

About This Post

SEO Recommendations:

- **Primary keyword:** "Nextcloud file sharing" — used in headline and early body copy
- **Related keywords to use:** "Nextcloud backup", "private cloud storage", "Nextcloud vs Google Drive", "self-hosted cloud storage", "GDPR compliant cloud storage"
- **Meta description (under 160 chars):** "Discover what Nextcloud is, why it's a privacy-first alternative to Google Drive and Dropbox, and how Tranquil IT can set it up for you."
- **Internal linking opportunity:** Link to the Mac and Windows backup guides, and any Tranquil IT service pages for hosted solutions
- **External linking opportunity:** Nextcloud's official website (nextcloud.com), GDPR information pages
- **Image alt text suggestion:** "Nextcloud dashboard showing file storage and sharing interface on a laptop screen"

Suggested URL Slug - /blog/what-is-nextcloud

Our Recommended Password Managers (And Why You Should Be Using One)

Be honest — how many of your passwords are some variation of the same thing? Maybe you swap out a number at the end, or add an exclamation mark to satisfy the "must include a symbol" requirement. You're not alone. Most people do it, and most people have no idea how much risk that creates.

If one of your accounts gets compromised — and data breaches happen constantly — attackers will try that same password everywhere. Your email. Your bank. Your work accounts. A single weak link can unravel everything.

The good news is that fixing this is genuinely easy, and you only have to remember one password to do it. That's the whole point of a password manager. Here at Tranquil IT, we recommend them to every single one of our customers, and we use them ourselves. Let's break down what they are and which ones we think are worth your time.

What Is a Password Manager?

A password manager is an app that stores all of your passwords in a secure, encrypted vault. Instead of trying to remember dozens of different logins, you remember one strong master password to unlock the vault — and the app handles everything else.

Most password managers will also:

- **Generate strong, unique passwords** for every account you create
- **Autofill your login details** on websites and apps so you don't have to type anything
- **Sync across all your devices** — your phone, laptop, tablet, all of it
- **Alert you if your passwords have been compromised** in a known data breach
- **Store more than just passwords** — secure notes, card details, addresses, and more

Once you've used one for a week, you'll wonder how you ever managed without it.

Our Top Recommendation: 1Password

Best for: individuals, families, and businesses who want the complete package

1Password is the password manager we use at Tranquil IT, and it's the one we recommend most confidently to our customers. It's been around since 2006, has an excellent reputation for security, and manages to be both powerful and genuinely easy to use — which isn't always an easy balance to strike.

What makes 1Password stand out

Watchtower is one of 1Password's best features. It continuously monitors your saved passwords and alerts you if any have been exposed in a data breach, are weak or reused, or if any of your accounts support two-factor authentication that you haven't switched on yet. It's like having a security advisor built into your password manager.

Travel Mode is something you won't find in most competitors. It lets you temporarily hide selected vaults when crossing borders — useful for business travellers who don't want sensitive company data accessible if a device is inspected.

Passkey support means 1Password is ready for the future of authentication. Passkeys are replacing traditional passwords on many major platforms, and 1Password handles them seamlessly alongside your regular logins.

Business and team features are where 1Password really shines for companies. You can share credentials securely between team members, set access permissions, and manage everything from a central admin dashboard. It's one of the cleanest implementations of team password management available.

The basics

- Apps for Windows, Mac, iOS, Android, Linux, and all major browsers
- End-to-end encryption — 1Password cannot see your passwords, ever
- Offline access to your vault when you don't have internet
- Family plans that let you share selected passwords with household members

Pricing: From around £2.65/month per person (individual), with family and business plans available.

Also Recommended: NordPass

Best for: users who want simplicity and are already in the Nord ecosystem

NordPass comes from the team behind NordVPN, and it brings the same focus on clean design and ease of use that Nord is known for. It's a strong, reliable password manager that's particularly well-suited to users who want something straightforward without a lot of complexity.

What NordPass does well

Data breach scanner checks your email addresses against known breaches and lets you know if any of your stored passwords have been exposed — handy for staying one step ahead of threats.

Password health checker gives you a clear overview of your weak, old, or reused passwords so you know exactly where to focus your attention.

Secure sharing lets you share passwords and notes with other NordPass users without ever revealing the actual password — useful for households or small teams.

Email masking is a newer feature that lets you create throwaway email addresses for sign-ups, keeping your real inbox and identity protected.

The basics

- Apps for Windows, Mac, iOS, Android, Linux, and all major browsers
- Zero-knowledge architecture — NordPass staff cannot access your vault
- Biometric login (Face ID, fingerprint) on mobile
- Free tier available with limited features

Pricing: Free plan available; premium from around £1.49/month per person.

Also Recommended: Bitwarden

Best for: privacy-conscious users and those who want an open-source option

Bitwarden is the open-source option on our list, and that matters more than you might think. Because its code is publicly available, independent security researchers around the world can — and do — inspect it for vulnerabilities. There's nowhere to hide anything, which is about as trustworthy as software gets.

It's also the most flexible option here, and one of the most affordable.

What Bitwarden does well

Open-source and independently audited means you're not just taking a company's word for it that your data is safe. The code is transparent, and Bitwarden undergoes regular third-party security audits.

Self-hosting option is a big deal for privacy-conscious users and businesses. If you'd rather not store your vault on Bitwarden's servers, you can run your own instance — similar in principle to the way Nextcloud gives you control over your own file storage.

Generous free tier includes unlimited passwords on unlimited devices, which is more than most competitors offer for free. For many personal users, the free version is all they'll ever need.

Send is a useful feature that lets you securely share encrypted text or files with anyone — even people who don't use Bitwarden — via a temporary link.

The basics

- Apps for Windows, Mac, iOS, Android, Linux, and all major browsers
- End-to-end encryption with zero-knowledge architecture
- Full-featured free tier (unlimited passwords, unlimited devices)
- Premium features — breach monitoring, advanced 2FA — from £0.83/month

Pricing: Free plan available; premium from around £0.83/month per person.

How They Compare at a Glance

Feature	1Password	NordPass	Bitwarden
Free tier	No (14-day trial)	Yes (limited)	Yes (full-featured)
Open source	No	No	Yes
Self-hosting	No	No	Yes
Travel Mode	Yes	No	No

Feature	1Password	NordPass	Bitwarden
Passkey support	Yes	Yes	Yes
Breach monitoring	Yes	Yes	Yes
Business/team plans	Yes (excellent)	Yes	Yes
Our recommendation	Top pick	Great for simplicity	Best open-source option

---

Which One Is Right for You?

If you're not sure where to start, here's the short version:

Choose 1Password if you want the best overall experience, particularly if you're a business or need to share passwords across a team. It's the one we use and trust most.

Choose NordPass if you want something clean and simple, already use NordVPN, or are looking for an easy entry point into password management.

Choose Bitwarden if you're privacy-focused, want open-source software you can verify yourself, or need the flexibility of self-hosting — and especially if budget is a consideration.

Whichever you choose, using any password manager is a massive improvement over reusing the same passwords everywhere. It's one of the single most impactful things you can do for your online security.

Need Help Getting Set Up?

If you'd like help choosing the right password manager for your household or business, or you need support rolling one out across your team, the Tranquil IT team is happy to help. Get in touch at support@tranquilit.net or give us a call on 01279 658331.

SEO Recommendations:

- **Suggested URL slug:** `/blog/best-password-managers`
- **Primary keyword:** "best password managers" — used in headline options and body copy
- **Related keywords to use:** "1Password review", "NordPass vs Bitwarden", "password manager for business", "what is a password manager", "secure passwords"
- **Meta description (under 160 chars):** "Tranquil IT's recommended password managers — 1Password, NordPass, and Bitwarden — explained simply so you can find the right one

for you."
- **Internal linking opportunity:** Link to the Mac backup guide, Windows backup guide, and Nextcloud guide to build out the security series
- **External linking opportunity:** 1Password, NordPass, and Bitwarden product pages
- **Image alt text suggestion:** "Password manager app open on a smartphone showing a secure vault"

Suggested next steps:

- Add affiliate or referral links to each product if applicable
- Consider a follow-up post: "How to Switch to a Password Manager in 5 Steps"
- This post pairs well with a piece on two-factor authentication as part of a broader cybersecurity series

IT Equipment Recycling UK: Why Your Old Tech Doesn't Just Disappear

IT Equipment Recycling UK: Why Your Old Tech Doesn't Just Disappear

Published: 2 April 2025 | **Reading time:** 6 min | **Category:** E-Waste Guides

> The UK generates 1.65 million tonnes of e-waste every year — and 12 million computers have ended up in landfill in the last 5 years alone. Here's why that matters, and exactly what you can do about it.

Table of Contents

Key Statistics at a Glance

Stat	Figure	Source
UK e-waste generated per year	**1.65 million tonnes**	UN Global E-Waste Monitor 2024
Computers & laptops sent to landfill (last 5 years)	**12 million devices**	Collect and Recycle
UK e-waste NOT properly recycled	**~55%**	WRAP UK
IT & telecoms waste annually	**~38,000 tonnes**	Uswitch / GOV.UK
E-waste generated per person per year	**24.5 kg**	UN Global E-Waste Monitor 2024

1. The Scale of the Problem

When you upgrade your phone or replace an old PC, what happens to the old one? For millions of people in the UK, the answer is: it ends up in a bin, a cupboard, or eventually a landfill.

The UK is one of the biggest producers of electronic waste in the entire world — generating around **24.5 kg of e-waste per person, per year**. That's roughly the weight of a large microwave, every single year, for every single person in the country.

IT equipment specifically — laptops, desktops, monitors, phones, tablets, printers, and routers — makes up a significant and growing chunk of that figure. IT and telecoms waste has **nearly doubled over the last 15 years**, rising from around 19,000 tonnes in 2008 to almost 38,000 tonnes annually today.

> **Around 12 million computers and laptops** have ended up in UK landfill in the past five years alone. That's millions of devices packed with metals, chemicals, and recoverable materials — buried in the ground instead of being reused or recycled.

2. What Happens When Electronics Go to Landfill?

Electronics aren't like food scraps or cardboard — they don't break down harmlessly. Inside your old laptop or phone are materials like **lead, mercury, and cadmium**. When these devices are buried in landfill, those toxic substances slowly leak into the surrounding soil and water over years and decades.

The damage isn't abstract. It affects farmland, rivers, drinking water, and wildlife. It's a slow-burning environmental crisis happening underneath our feet.

Environmental impacts of e-waste in landfill

- **Soil contamination** — heavy metals from circuit boards and batteries seep into the ground, making land toxic and unusable for agriculture
- **Water pollution** — chemicals leach into groundwater and rivers, threatening ecosystems and drinking water supplies
- **Air pollution** — in developing countries where much UK e-waste is illegally exported, devices are often burned to extract metals, releasing toxic fumes
- **Wildlife harm** — contaminated environments devastate local animal and plant populations
- **Lost resources** — valuable materials like gold, silver, and copper are buried forever instead of being recovered and reused

---

> ⚠ **Did you know?** One tonne of old circuit boards contains up to **300 grams of gold** — that's 60 times more concentrated than gold ore mined from the earth. The UN estimates recoverable materials in global e-waste are worth approximately **$57 billion annually**. By throwing electronics away, we're literally burying treasure.

---

3. The Data Security Risk

This one often gets overlooked. When you throw away an old device without properly wiping it, your data goes with it. ICO research shows the majority of discarded devices contain residual personal data — passwords, documents, photos, banking details, and login credentials.

Simply deleting files or doing a basic factory reset is often **not enough**. A professional IT recycling service will ensure your data is securely and completely destroyed before the device is processed — protecting you as well as the planet.

For businesses, this isn't just good practice — it's a legal requirement under **UK GDPR**. Improper disposal of devices containing customer or employee data can result in serious fines from the ICO.

---

4. UK Recycling by the Numbers

Here's the uncomfortable truth: the amount of electronic equipment sold in the UK grew by **25% between 2018 and 2024**. But the amount being properly collected and recycled? It barely moved — rising by less than 1% in the same period.

> "*Only 45% of UK e-waste is formally recycled. More than half of all our discarded electronics are not handled properly.*"

How the UK Compares Internationally

Country	E-Waste Per Capita	Formal Recycling Rate	Notes
Norway	26 kg/person	~44%	Take-back scheme in place
UK	**24.5 kg/person**	**~45%**	Improving, but gap remains
Switzerland	23.4 kg/person	>50%	Take-back scheme in place
Global Average	~7 kg/person	17.4%	Well below target

Sources: UN Global E-Waste Monitor 2024, WRAP UK, Uswitch

---

5. How to Recycle Your IT Equipment

The good news? There are clear, accessible ways to dispose of your old tech responsibly. Here's exactly how:

Step 1 — Find your nearest WEEE drop-off point

Most local councils and many large retailers — Currys, John Lewis, Argos — accept old electrical items for free recycling. Use the official finder at recycleyourelectricals.org.uk to find your closest point.

Step 2 — For businesses: use a certified IT recycler

UK businesses are legally required to dispose of IT equipment through a licensed waste carrier under the WEEE Regulations 2013. A certified WEEE recycler will collect your equipment, issue a duty of care certificate, and handle secure data destruction.

Step 3 — Consider donating if the device still works

Working laptops and computers can be refurbished and donated to schools, charities, and community groups. Organisations like **Computer Aid** and **Donate a PC** give devices a meaningful second life.

Step 4 — Don't forget the smaller items

Phones, cables, earphones, routers, keyboards — these all count as e-waste too. Many mobile retailers offer phone take-back schemes, and most supermarkets now have small electricals recycling bins near the entrance.

Step 5 — Think before you buy

Choose brands that offer take-back schemes or use recycled materials. Extending the life of a device by even one extra year reduces its carbon footprint significantly — manufacturing new electronics is enormously energy-intensive.

6. Frequently Asked Questions

How much IT equipment ends up in landfill in the UK? Around 12 million computers and laptops have ended up in UK landfill over the past five years. The UK generates approximately 1.65 million tonnes of total e-waste every year, making it the second-largest e-waste producer per capita in Europe at around 24.5 kg per person annually.

Is it illegal to throw IT equipment in the bin in the UK? Yes — for businesses, it is a legal requirement under the WEEE Regulations 2013 to dispose of electrical and electronic equipment through a licensed waste carrier. For households, e-waste should be taken to designated WEEE collection points rather than placed in general bins or black bag waste.

Where can I recycle old IT equipment for free in the UK? You can recycle IT equipment free of charge at your local council household waste recycling centre, through large retailers like Currys or John Lewis, or via the drop-off finder at recycleyourelectricals.org.uk. Businesses should contact a certified WEEE recycler for collection.

What percentage of UK e-waste is actually recycled? Only around 45% of UK e-waste is formally recycled through proper channels. The remaining 55% ends up in landfill, is illegally exported, or is otherwise improperly disposed of. WRAP estimates the UK could realistically achieve 65–70% recycling with improved infrastructure and greater business compliance.

Is my data safe when I recycle my old computer? Not automatically. Simply deleting files or factory resetting a device is often not enough to permanently erase data. A certified IT recycler or WEEE specialist will carry out secure data destruction — either through certified software wiping or physical shredding of drives — and provide documentation confirming it has been done.

One Device. One Decision. Real Impact.

You don't need to be an environmental expert. You just need to make a different choice the next time you're done with a device.

□□ Find a drop-off point near you → recycleyourelectricals.org.uk

SEO Metadata (for your CMS)

- **Meta title:** IT Equipment Recycling UK: Why Your Old Tech Doesn't Just Disappear | E-Waste Guide 2025
- **Meta description:** The UK generates 1.65 million tonnes of e-waste every year — and 12 million computers have ended up in landfill in the last 5 years alone. Learn why recycling your IT equipment matters, and exactly how to do it.
- **Focus keyword:** IT equipment recycling UK
- **Secondary keywords:** e-waste UK, recycle old laptop UK, WEEE recycling, computer recycling UK, how to recycle electronics UK, IT disposal UK
- **Canonical URL:** https://yourdomain.co.uk/it-equipment-recycling-uk
- **Article type:** Educational / Awareness
- **Schema types:** Article, FAQPage, BreadcrumbList

Data sources: UN Global E-Waste Monitor 2024 · WRAP UK · Material Focus · GOV.UK WEEE Statistics · ICO Research 2024

Sharing this article could save a device from landfill. Please pass it on. ♻