IT Checklist for Buy4Tradies Members

BUY4TRADIES
STRONGER TOGETHER

In today's digital world, it's more important than ever to make sure your business is set up with reliable, secure, and well-managed technology.

This simple checklist is designed to help Buy4Tradies members quickly assess the current state of their IT setup and identify areas that might need attention.

Not every item will apply to every business—but going through the list is a great way to spot gaps, reduce risks, and stay on top of your tech.

For each question below, tick either: **Yes**, **No**, or **I Don't Know**.

This will help highlight what's working well and where you might need to take action.

DISCLAIMER:

It's OK if you don't know the answer to something, but ask yourself: does someone in your business know? If no one does, that might be a sign it needs attention.

Reach out to the Buy4Tradies team so that can assist and point you in the right direction to ensure we get things right.

1. Internet & Network Setup

A fast, secure, and reliable internet connection is the backbone of your business operations. Proper setup helps avoid downtime, protects against cyber threats, and keeps your team connected.

Risk if ignored: Poor connectivity leads to lost productivity, while weak network security can leave your business open to cyberattacks or data theft.

Question	Yes	No	I Don't Know
• Do you have a reliable modem/router (preferably business-grade)?	☐	☐	☐
• Is your Wi-Fi secured with WPA2 or WPA3 encryption? • **WPA2** and **WPA3** are types of Wi-Fi security used to protect your wireless network from unauthorised access. Both require a password to join the network, but WPA3 adds stronger encryption and better safeguards, making it the preferred choice for modern routers.	☐	☐	☐
• Do you use a network switch if you have multiple wired devices? • A **network switch** is a device that connects multiple wired devices (like computers, printers, or security cameras) within the same network so they can communicate with each other. Think of it like a power board, but for internet cables.	☐	☐	☐
• Are desktops and printers connected with Ethernet cables where possible?	☐	☐	☐
• Do you have a battery backup for critical devices like the modem or server in case of power outages?	☐	☐	☐
• Are all devices and cables clearly labelled?	☐	☐	☐

2. Computers & Devices

Modern, well-maintained devices keep your team productive and reduce the risk of crashes, security holes, or costly replacements.

Risk if ignored: Old or unmaintained computers are slower, crash more often, and are more vulnerable to viruses and cyber threats.

Question	Yes	No	I Don't Know
• Are all computers under 5 years old?	☐	☐	☐
• Are all computers running a supported operating system?	☐	☐	☐
• Does each user have their own dedicated computer?	☐	☐	☐
• Are all operating systems and drivers regularly updated?	☐	☐	☐
• Are admin and standard user accounts separated (non-admin for everyday use)?	☐	☐	☐
• Is device encryption enabled (e.g., BitLocker on Windows or FileVault on Mac)? • **Device encryption** is a security feature that scrambles the data on your computer or device so that no one can read it without the correct password or login.	☐	☐	☐
• Do you keep an inventory list with model numbers, serial numbers, and purchase dates?	☐	☐	☐

3. Cybersecurity Basics

Protecting your systems from viruses, scams, and hackers is essential to keep your data safe and your business running smoothly.

Risk if ignored: A single cyberattack can cost your business thousands, damage your reputation, or even shut you down temporarily or permanently.

Question	Yes	No	I Don't Know
• Is antivirus or antimalware software installed and active on all devices?	☐	☐	☐
• Is a firewall enabled on every device? • A **firewall** is a security feature that acts like a barrier between your device or network and the internet. It controls what data can come in or go out, helping block hackers, viruses, or suspicious activity.	☐	☐	☐
• Have you changed the default passwords on your router or modem?	☐	☐	☐
• Are you using a password manager for your team? (eg. Keeper)	☐	☐	☐
• Do you enforce strong password rules?	☐	☐	☐
• Is two-factor authentication (2FA) turned on for important accounts (email, cloud storage, banking)?	☐	☐	☐
• Have users been trained to recognise phishing and scam emails?	☐	☐	☐

4. Email & Cloud Services

Using secure, centralised email and file storage keeps communication professional, organised, and protected, whilst making it easier to collaborate and access work from anywhere.

Risk if ignored: Personal or unsecure systems are more prone to hacks, lost data, and confusion over who has access to what.

Question	Yes	No	I Don't Know
• Are you using a business email system like Google Workspace or Microsoft 365?	☐	☐	☐
• Are you avoiding personal or unsecure email setups like Gmail, IMAP, or POP accounts? • **IMAP (Internet Message Access Protocol)** and **POP (Post Office Protocol)** are older methods of receiving email, often used with personal or basic email setups. Both can lack the advanced security, syncing, and management features of modern business email platforms like **Google Workspace** or **Microsoft 365**.	☐	☐	☐
• Are you storing files in the cloud using a secure service (e.g., Google Drive, OneDrive, Dropbox Business)?	☐	☐	☐
• Are file and folder permissions set so users only access what they need?	☐	☐	☐
• Do you have a record of all email accounts, logins, and assigned roles?	☐	☐	☐

5. Data Backup & Recovery

Accidents happen. Regular backups make sure you don't lose important data, and help you get back up and running quickly if something goes wrong.

Risk if ignored: If your data is lost or held hostage by ransomware and you don't have a backup, it may be unrecoverable, potentially costing your business greatly.

Question	Yes	No	I Don't Know
• Is important data backed up locally daily?	☐	☐	☐
• Is important data backed up to the cloud daily?	☐	☐	☐
• Do you test your backups at least once a month?	☐	☐	☐
• Are all critical items backed up, such as client files, financials, settings, and emails?	☐	☐	☐
• Do you have a written disaster recovery plan (even a simple one)? • This is a step by step guide outlining what you need to do to quickly recover and continue running after unexpected events like cyber-attacks or natural disasters.	☐	☐	☐

6. Support & Maintenance

Having someone responsible for your tech and doing regular upkeep prevents problems before they happen and ensures things run efficiently and you stay up to date.

Risk if ignored: Small issues can turn into big, expensive problems without proactive attention, and no one may know what to do when things go wrong.

Question	Yes	No	I Don't Know
• Is someone responsible for your IT (internally or externally)?	☐	☐	☐
• Do you track and renew software licenses on time?	☐	☐	☐
• Is regular maintenance scheduled (updates, clean-up, performance checks)?	☐	☐	☐
• Do you have clear instructions for setting up a new device or user?	☐	☐	☐
• Are your printer and accessories working, with drivers and firmware up to date?	☐	☐	☐

7. Compliance & Policies

Clear rules around device use, internet access, and customer data help protect your business legally and create a safer, more consistent work environment.

Risk if ignored: You could face legal issues, fines, or customer complaints if data is mishandled or misused.

Question	Yes	No	I Don't Know
• Do you have a basic acceptable use policy for company devices and internet?	☐	☐	☐
• Are there clear rules for how devices and the internet should be used?	☐	☐	☐
• Is there a checklist for onboarding staff?	☐	☐	☐
• Is there a checklist for offboarding staff?	☐	☐	☐
• Do you have a policy for handling customer data securely?	☐	☐	☐
• Do you maintain a basic IT manual with login details, backup steps, and key contacts?	☐	☐	☐

8. User Management

Controlling who has access to what protects sensitive information and reduces the risk of mistakes or breaches, especially when staff leave.

Risk if ignored: Forgotten accounts, shared logins, or over-permissioned users can lead to unauthorised access, data leaks, or security breaches.

Question	Yes	No	I Don't Know
• Does each user have their own log in to various software so you can track who has done what?	☐	☐	☐
• Are user accounts deactivated immediately when someone leaves the company?	☐	☐	☐
• Do users only have access to the tools and files they actually need?	☐	☐	☐

9. Email & Domain

Using a professional email tied to your business domain builds trust with customers and improves your email security.

Risk if ignored: Free or personal emails can look unprofessional, get flagged as spam, and are more easily spoofed by scammers.

Question	Yes	No	I Don't Know
• Are you using a custom domain for email (e.g., yourname@yourbusiness.com)?	☐	☐	☐
• Have SPF, DKIM, and DMARC records been set up for your email domain? • **SPF**, **DKIM**, and **DMARC** are security settings for your business email domain that help stop scammers from sending fake emails pretending to be you. Together, they protect your domain from being used in email spoofing or phishing attacks, and help your emails avoid being marked as spam.	☐	☐	☐
• Is spam and phishing protection active on your email system? (Usually included with Google Workspace or Microsoft365)	☐	☐	☐

10. Ongoing Maintenance

Regular check-ups on your systems ensure everything stays secure, up to date, and cost-effective, saving time, money, and stress in the long run.

Risk if ignored: Ignored systems slowly degrade, security gaps go unnoticed, and costs creep up due to poor planning or unexpected failures.

Question	Yes	No	I Don't Know
• Do you check backups, software updates, and antivirus status monthly?	☐	☐	☐
• Do you review software subscriptions and overall security every 3 months?	☐	☐	☐
• Do you plan and budget annually for IT hardware, software, and support?	☐	☐	☐