

How to create a BYOD policy

If your team is using personal phones, tablets or laptops for work—even just to check email—you need a clear bring your own device (BYOD) policy.

Our worksheet is designed to help you define what that looks like for your business. It'll guide you through the decisions that matter—from who can use personal devices and what for to how you'll keep company data secure.

Use this space to map out your thinking and draft your policy from scratch—based on how your business actually works.

Please note that as all businesses are different, this is designed only as an overview, and not an exhaustive list.



How to create a BYOD policy

1) Set your objectives

Before writing any rules, clarify why a BYOD policy is important for your business. What are your main goals?

- Are you trying to save money?
- Support flexible working?
- Improve employee experience?
- Boost recruitment and retention?
- Meet compliance obligations?
- Is BYOD a short-term solution or a long-term strategy?
- What does success look like?

2) Assess user needs

Who needs BYOD access and what for? This helps you set scope and permissions based on real needs.

- Which people or roles need access to business systems and why? (sales team needing mobile access, designers using personal high-spec programmes etc.).
- What kind of devices will they use (phones, tablets, laptops)?
- What tasks will they need to complete? (checking email, accessing cloud documents, using specific business apps, joining video calls etc.)

3) Identify the risks

Where are the weak points and how will you tackle them? This section is for spotting the risks that come with BYOD and planning ahead.

- What's your most sensitive business or customer data that could be at risk? (customer details, financial records, intellectual property etc.).
- What company information or systems will people access? (Be specific: CRM, accounting software, shared drives, email, messaging tools etc.).
- Will personal devices be used for client interactions or handling sensitive client data? If so, how?
- Could personal devices expose you to phishing, malware or data breaches?
- What compliance obligations (like GDPR or industry-specific rules) apply to your data and how could BYOD affect them?

- What happens if a personal device containing company data is lost or stolen? (remote wipe capabilities, immediate reporting etc.).
- What are BYOD's biggest security concerns (unsecure home Wi-Fi, employees installing risky apps etc.)

4) Setting the policy rules

What's allowed, what's not, and what happens if it goes wrong? Use this section to draft the building blocks of your BYOD policy.

- Which devices are allowed, which aren't, and why? (only those with up-to-date operating systems or automatic security updates, no refurbished devices or those unsupported by provider security etc.).
- Will you need specific protection ? (antivirus, password manager, VPN, Mobile Device Management etc.).
- Do the devices need to be registered with IT?
- How will you handle data storage, access and sharing?
- What happens if someone loses a device or breaks the rules?
- What happens if someone leaves the company?
- Will you reimburse your team for using their personal devices? (data plans, internet charges, specific apps etc.)

5) Plan your rollout

How will you launch the policy and get people on board? A policy is only effective if everyone understands and follows it.

- How will you introduce the policy and explain it clearly? (team meetings, written documents, intranet, training sessions etc.).
- Who needs training or support to follow the rules?
- What's the planned timescale? (phased approach by department or team, immediate company-wide implementation).
- How will you ensure ongoing compliance?
- How and how often will you update or revisit it as your business grows?

What's next?

Once you've mapped out your thinking, you're ready to write your full bring your own device BYOD policy. Remember, it's about balancing flexibility with robust security—so it fits your business, your systems and your people.

If you have any questions or need help putting it all together, our expert [V-Hub Digital Advisers](#) are on hand for personalised, 1-2-1 support.