Device Management for Remote Staff: A UK SME Guide

Executive Summary

- Using remote and hybrid working methods creates greater flexibility; however, without sufficient security and control, these methods place additional cybersecurity risk onto your business.
- In fact, most small to medium-sized enterprises' (SMEs) recent breaches in the UK occurred as a result of compromised laptop, mobile devices or stolen credentials.
- To ensure that every work device is as secure as possible, it is important to have an effective device management strategy that encompasses secure device configurations (e.g., updated, encrypted) and the ability to remotely control devices.
- Basic security controls such as multi-factor authentication (MFA) or automatic updates and encrypting your hard drive can greatly reduce cybersecurity risks to your SME.
- When it comes to Bring Your Own Device (BYOD) policies, clarify your expectations with employees instead of making assumptions.
- The UK General Data Protection Regulation (GDPR) places a duty on your business to protect the personal data of your employees regardless of the type of device they are using.
- SMEs can take advantage of several cost-effective solutions that provide centralised device management capabilities without an enterprise-level budget.
- Develop a simple 30-day plan that will significantly improve your remote security.

Who This Guide Is For

This high-level overview of managing remote security for SMEs will provide you with the knowledge and experience necessary to make informed decisions about:

- UK SMEs (1-50 employees)
- Owner/Managed businesses
- Administrative staff responsible for managing remote teams
- Financial staff with oversight of IT functions
- Management decisions regarding hybrid working with little or no technical background required.

What You'll Achieve

By completing this guide, you will:

- Comprehend device management defined clearly in layman's terms
- Recognise the most typical dangers associated with devices that are remote
- Familiarise yourself with the minimum acceptable levels of protection required for UK-based small businesses
- Become acquainted with the dangers involved with using personal owned devices at work (BYOD) and how to establish policies regarding the use of these devices

- Have improved compliance with GDPR laws regarding mobile workers
- Have a 30-day plan to implement improved device management

What Is Device Management?

Device management refers to:

- The management and security of laptops, desktops, tablets, and mobile phones that are used during the course of one's work.

This includes the following:

- Keeping devices current/updated
- Enforcing security policies on devices
- Installing EDR/antivirus programs on devices
- Enabling device encryption
- Controlling/monitoring user access to devices
- Remotely locking/changing password or wiping a device
- Monitoring compliance with your organisation’s device management policies

In layman's terms, if the device can access company data, it must be managed.

Why Device Management Matters in 2026

All employees of UK small businesses usually work in a hybrid work environment.

Employees frequently do the following:

- Work from home
- Use public Internet Wi-Fi to access resources
- Access Cloud services with personal devices
- Store sensitive company information on their own devices

According to the National Cyber Security Centre (NCSC) organisations should consider remote devices part of the organisation’s corporate network.

The Information Commissioner's Office (ICO) has clearly stated that if a laptop that has personal information on it is stolen or loses its password protection it will become a breach of the UK GDPR and is therefore reportable under UK regulations.

If your device has been lost or stolen and/or you have lost the ability to protect the data that is on your device, report the breach to the NCSC immediately.

Risks of Unmanaged Remote Devices

1) Lost or Stolen Laptops

Example:

- A manager is travelling and accidentally leaves their laptop on a train. It has no encryption and can be used by anyone who finds it for access to customer data.

Risk:

- A notification to the ICO, and damage to the company's reputation, as well as the possibility of being fined.

2) Unpatched Devices:

- Remote workers are not updating their devices and, in many cases, are using devices that have known vulnerabilities and could potentially be used against them such as by ransomware.

3) Personal Devices Accessing Corporate Data:

Without controls in place:

- Data is copied to personal online storage; or,
- Employees are using unsecured Wi-Fi connections at home; or,
- Employees do not have antivirus software on their personal devices.

4) Weak Passwords and No MFA:

- If an employee's username/password has been compromised, the hacker has access to company systems.

5) No Remote Wipe Capability:

- If a device is lost, you have no way to erase corporate information from that device.

Core Device Management Standards

1. Device Inventory & Visibility

What it is

- The company maintains a record of each device accessing its systems.

Why it matters

- Visibility is a prerequisite to securing any device.

Minimum level

- A spreadsheet of all issued devices
- A list of serial numbers
- A record of each user assigned to the device

Better level

- Centralised device management solution
- Ability to register devices automatically

Quick wins

- Create device register
- Identify any unlicensed devices accessing email
- Remove any devices with no known ownership

2. Automatic Updates & Patch Management

What it is

- Having devices automatically download/install security updates.

Why it matters

- Cyber criminals typically exploit known or documented vulnerabilities.

Minimum level

- Enable automatic updates on supported MacOS/Windows PCs.
- Ensure that mobile operating systems are configured to automatically update.

Better level

- Centralised update management solution
- Reporting on the number of compliant devices

Quick wins

- Check whether devices run a supported OS
- Remove outdated applications
- Configure PC/Mac devices to automatically restart when updating.

3. Antivirus / EDR Protection

What it is

- Endpoint security software that identifies malware and maliciously-acted-upon behaviour.

Why it matters

- Remote devices do not have the protection of office firewalls

Minimum level

- Business Class/Grade Antivirus on all the laptops

Better level

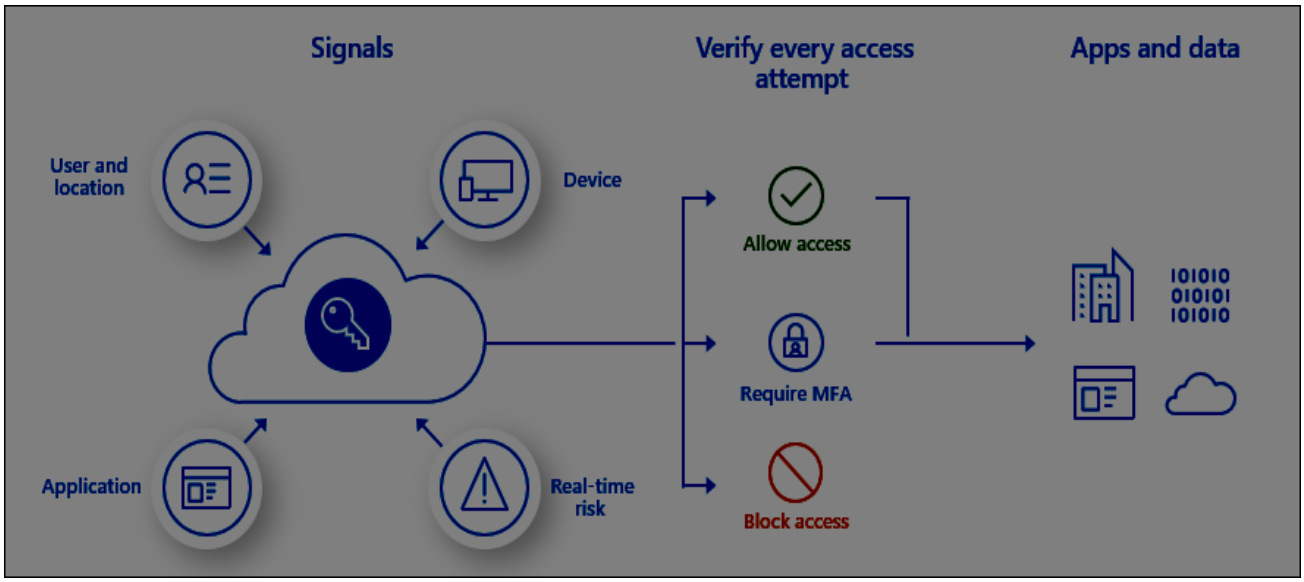
- Managed EDR with Monitoring Alerts

Quick wins

- Check Protection is active on all devices
- Remove Free Consumer-Grade Antivirus

- Confirm that Automatic Signature Upgrades are Working

4. Multi-Factor Authentication (MFA)



What it is

- Extra verification beyond just a password

Why it matters

- Prevents most account takeovers

Minimum level

- MFA enabled for email and cloud apps

Better level

- Having Conditional Access Rules where, the ability to approve users is based upon whether or not their device is compliant

Quick wins

- Require MFA for all users
- Disable Legacy Authentication Methods
- Use Authenticator Apps vs. SMS

5. Device Encryption

What it is

- The encryption of hard-drives, making it so that the data cannot be retrieved if the device is stolen

Why it matters

- Physically protecting data.

Minimum level

- Use BitLocker or FileVault

Better level

- Centrally Managed Encryption Keys

Quick wins

- Confirm Encryption Status
- Securely Store Recovery Keys
- Encrypt USB Storage Devices

6. Remote Lock & Wipe

What it is

- The ability to lock or erase a device from a remote location.

Why it matters

- It reduces the risk associated with lost devices.

Minimum level

- Remote wipe capability on mobile devices.

Better level

- Full remote wipe capability through MDM for laptops.

Quick wins

- Test remote wipe function on one device
- Confirm mobile device has remote wipe capability
- Remove access immediately when an employee terminates their employment with your organisation.

7. Monitoring & Compliance Reporting

What it is

- Verifying the security posture of each device.

Why it matters

- Security is an ongoing process not just a one-time effort; you will need to continually monitor devices for compliance.

Minimum level

- Device review on a quarterly basis.

Better level

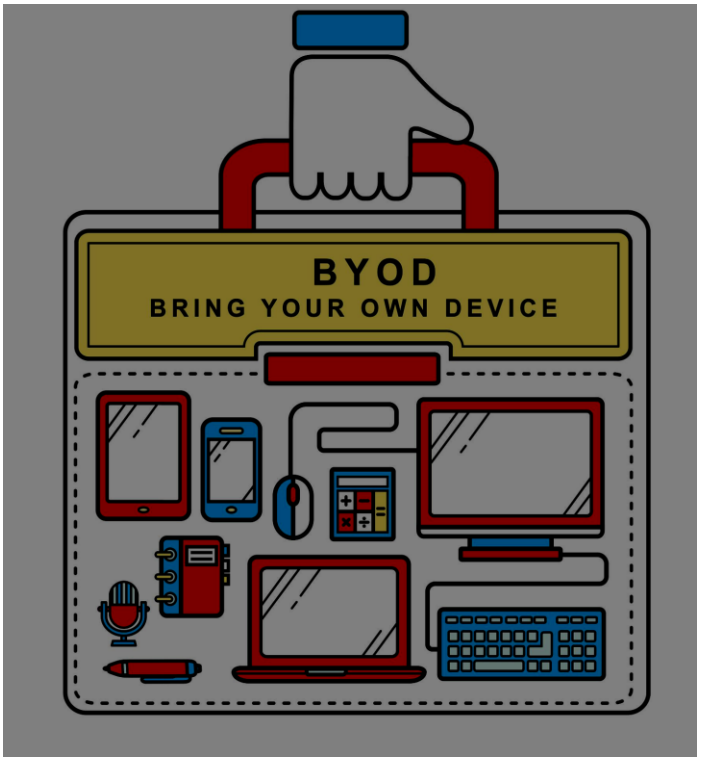
- Automated compliance alerts.

Quick wins

- Schedule a device audit every 3 months
- Review administrator access / permissions
- Disable all accounts that have been inactive for the last 90 + days

BYOD (Bring Your Own Device) Considerations

Some organisations allow employees to bring their own devices to work (e.g., smartphones, tablets), increasing the overall risk to the organisation. When developing policies, companies should take the following into consideration:



Minimum BYOD Policy Should Include:

- Multi-Factor Authentication (MFA) usage will be mandatory.
- Local storage of company data will be prohibited.
- All devices used must have data encrypted in accordance with company policy.
- All devices used must have a current antivirus program installed.
- All company data can and will be deleted when the company desires it.
- All lost devices must be reported immediately to the company's IT department.

Better Practice

- Utilising Mobile Device Management (MDM) Technology
- Separate Corporate From Personal Data
- Containerise Applications

Common BYOD Mistakes

- Establish A Written BYOD Policy
- Implement An Off boarding Process
- Create Company Based (And Employee Based) Visibility Of All Devices
- Require All Devices To Have Company Encrypted Data

30-Day Implementation Plan

Days 1–10 – Visibility & Basics
• Register Your Devices • Create Increased Security in Accessing Devices • Confirm All Devices Have Encryption Enabled • Remove Access from All Users Who Don’t Work Here Any more • Enable Automatic Device Updates
Days 11–20 – Strengthening Controls
• Implement Business Antivirus/EDR Software for All Devices • Start a Basic Mobile Device Management (MDM) Program • Implement Remote Wipe Capabilities on All Devices • Create a Written BYOD Policy
Days 21–30 – Governance & Monitoring
• Conduct Assessments to Determine What Devices Are in Use • Conduct Remote Wipe Testing • Create an Incident Response Plan • Train Employees on Device Security • Schedule Follow-Up Assessments on a Quarterly Basis

Frequently Asked Questions

- **Are personal devices secure to use at work?**

Yes; they can be if they have appropriate levels of controls.

- **Is encrypting difficult?**

No; there are many tools available that make encrypting easy.

- **Does Microsoft 365 manage devices, or does it require setup from you?**

Microsoft 365 will manage devices if you have set them up appropriately to do so.

- **What happens if an employee does not want to follow the policies regarding device controls?**

In order to enforce your policy you need a clear guideline as written into the employee's job description.

- **How often should I review devices?**

At least once every quarter.

- **Do I still need to use Antivirus on devices?**

Yes; an Antivirus program is necessary along with EDR and MFA for complete protection.

- **What should I do if I have lost my laptop?**

You should remotely wipe the laptop and change the password immediately.

- **Are remote devices at a higher risk than an office-based device?**

Yes; remote devices are at a higher risk than office-based devices, especially when connected to public Wi-Fi networks.

- **Is any Public Wi-Fi safe?**

No; Public Wi-Fi should only be used with an encrypted connection (VPN) and MFA enabled.

About This Guide

Computer Support Centre is a UK-based IT and cybersecurity consulting firm devoted to creating secure work environments for small and medium-sized businesses. For more than 15 years, we have used our extensive experience supporting UK businesses with respect to secure and efficient remote team management.

This guide embodies actual challenges that face businesses with 1 to 50 employees, particularly hybrid or fully remote work environments. We have created a list of practical and cost-effective controls that help decrease risk without introducing unnecessary complexity to your technology.

Our guidance uses UK best practices, including expectations under the UKGDPR, and guidance from the NCSC and the ICO. This guide has been written in straightforward language to help non-technical leaders in business make confident and educated decisions.

The mission of **Computer Support Centre** is simple (provide useful and actionable advice that increases the security of your business while facilitating business growth).

Conclusion

If you are a small business in the UK, managing your remote/hybrid devices does not need to be complex or costly. By implementing the essential components for securing devices (full-disk encryption, automatic updates, MFA on all accounts, a strong antivirus/EDR solution, remote wipe capabilities, and establishing written access policies/standards) you will close most of the common attack vectors used to target laptops and mobile devices that are outside of your office. If any employees use their own devices to conduct business, then simply implement a BYOD policy – that's the only consideration needed to protect your business at a reasonable level and meet the requirements of the Cyber Essentials scheme and UK GDPR, without impacting on your ability to perform daily activities. The top priority is to get the quickest, easiest wins from your 30-day checklist; turn on MFA and encryption this week and start building from there. These actions will allow you to effectively manage remote risks, protect client data, and simplify conversations with your chief financial officer about obtaining insurance or achieving compliance. You've got this small consistent actions will create strong security.