Managing Laptops for Remote Teams

Why managing remote laptops matters

- Small to medium sized businesses across the UK have adopted hybrid and/or remote working as normal practice.
- A good example of this is employees regularly using their laptops at home, in a café, at a client's office or even on public transport.
- It is important for employees to have well managed devices in order to allow them to carry out their job in as productive a manner as possible, whilst also protecting the company's data.
- If a device is poorly managed, it creates security risks as well as operational issues.
- If an employee loses their laptop or their laptop is stolen, there is a risk that the employee could have an unauthorised disclosure of sensitive data or have a loss of uptime for the business.
- Weak passwords or software that is out of date increases the risk of cyber-attacks.
- Using tools such as Microsoft 365, there are many different security controls that can be managed effectively in order to reduce the risks posed to SMEs who need to manage remote laptops effectively and securely while at the same time managing their own budgets.

Challenges of supporting remote and hybrid workers

Working with remote devices like laptops causes issues that working from the office doesn't. Here are a few of these issues listed below:

- Laptops are used in environment where users don’t have supervision (people use their own network at home, at a coffee shop, etc...)
- People who both work and play utilise the same equipment to conduct their daily tasks
- The IT department cannot assist users from the office in the same way they would if they were on-site.
- It is much easier to lose or have a laptop stolen than to have your equipment lost or stolen while at work.
- User’ computers receive updates and security patches more regularly when they are accessed from the office rather than when they are used remotely.

Key risks associated with remote laptops

These challenges create risks, however these risks can be mitigated with solid policies and tools to manage users' laptops' risk:

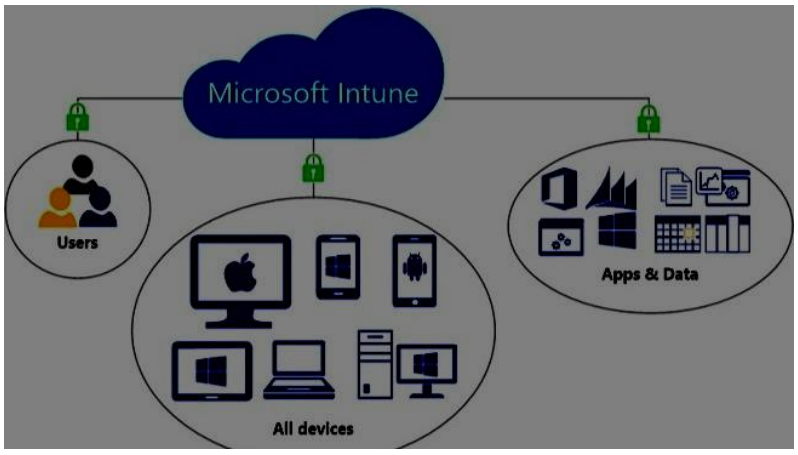
- Accounts can be compromised due to missing laptop's encryption or wipe features if lost or stolen
- Compromise because users are utilising home networks which have weak or no password identification
- Accounts can be compromised because software that is supposed to be patched with security flaw patches by the IT department are not up to date with 'as true production' software
- Accounts can be compromised due to weak passwords or no multi factor authentication (MFA)
- There is no back-up data when stored locally in case of device failure
- Unapproved applications (e.g. malware or other shadow IT) create an increased risk of potential compromise.

Each one of the above will increase the risk of a data breach, loss in productivity, and regulatory investigation (or similar) compliant with the UK's GDPR.

Best practices for managing laptops remotely

Centralised management of devices

- Leverage Microsoft Intune (includes with Business Premium) adoptions laptops, operating systems, and configurations, which enables you to push updates, apply encryption policies and securely delete lost devices through cloud management.



Full Disk Encryption

- Use full disk encryption to secure your data (by encrypting the entire drive)if your laptop gets lost or stolen. Windows users can use the BitLocker encryption feature. Mac users can utilise File Vault, which is functionality that comes with macOS.

Strong Password Policy

- Establish a strong password policy requiring at least 14 characters in length). If you are using multiple types of passwords, consider implementing a password manager/secure method password manager) and use unique passwords for each service/application. You typically do not want to be forced to change passwords more than once per month (unless they have been compromised).

Multi-Factor Authentication (MFA)

- To increase protection for your users and prevent most account breaches that result from stolen passwords, enable MFA for all company logins. This requires a second layer of verification (such as a code sent via SMS or a push notification from an app) prior to being able to access the user's account.

Automatic Software Updates

- Configure laptops to install security-related updates automatically as soon as they are available. This will help mitigate potential risks associated with vulnerabilities.

Endpoint Protection

- Utilise an endpoint protection solution such as Microsoft Defender (Free with Windows) or other 3rd SEDR) solution to help identify malware infections and other suspicious actions.

Secure Remote Access

- Utilise either a VPN or conditional access (Office 365) to securely access your company VDI system or to securely access your own LAN from a remote location.

Remote Device Lock and Erase

- Enrol devices in a manner that allows a user to remotely lock or erase (data) the device if lost or stolen.

Role Based Access Control

- Implement role based access management (RBAC) for all staff to ensure they only have access to the minimum amount of information to do their respective jobs.

Device security requirements

- All laptops owned by the company must be encrypted.
- Work accounts must use multi-factor authentication.
- Automatic updates should be turned on.
- Devices should have antivirus and endpoint detection & response (EDR) running.

- A password manager should be used.
- Devices that are lost or stolen should be reported within one hour.

Software and update management

- Configure your Windows operating system, Office productivity applications, web browsers, and third-party applications to use automatic updates.
- Major updates should be approved monthly using the software approval process.
- Remove all software that is no longer in use.
- Quick Win: Take a moment to check that you have configured your laptop to auto-update by going to "Settings > Update & Security".

Remote monitoring and support

- Use Intune or similar tools to remotely view the health of devices.
- Set up remote support tools (e.g., Team Viewer or Quick Assist) to help users.
- Monitor the login activity of users to detect any unusual patterns.
- Quick Win: Enable the Microsoft 365 risky sign-in alerts.

Laptop lifecycle and replacement planning

- Business Laptops have a lifespan of between 3 - 4 years.
- Business laptops should be replaced every 3 - 4 years to prevent loss of productivity from machines that may perform poorly or contain viruses/security threats.
- Laptops should be budgeted at £300 - £600 every four years for replacement. If you stagger replacement over four years, you will have a much easier time replacing them.
- Quick Win: Create a simple spreadsheet of all laptops, purchase date and estimated replacement date.

Staff responsibilities and acceptable use

- Use business equipment for sensitive work whenever possible.
- Report Stolen/Lost Equipment immediately.
- Follow the company password/MFA policy.
- Do not use public Wi-Fi for Company work requiring access to sensitive data (use a VPN if you must).
- Quick Win: Include a one-page guide to remote working in your employee handbook.

Remote laptop management checklist

- ✓ Are all company laptops encrypted?
- ✓ Have all work accounts been set up with MFA?

- ✓ Are automatic updates enabled?
- ✓ Is endpoint protection enabled?
- ✓ Have all devices been enrolled in your management tool (i.e., Intune)?
- ✓ Is remote wipe/lock enabled on devices?
- ✓ Is a password manager recommended?
- ✓ Is BYOD policy in place?
- ✓ Is there a documented procedure for reporting lost devices?
- ✓ Have quarterly audits been scheduled for devices?

Remote device security checklist

- ✓ Are strong passphrases being used?
- ✓ Is MFA being enforced for all logins?
- ✓ Are there no shared accounts?
- ✓ Are devices up to date?
- ✓ Are Antivirus/EDR running?
- ✓ Are public Wi-Fi networks avoided with regard to accessing sensitive work data?

Remote worker IT setup checklist

- ✓ Company laptop has been provided (if possible)
- ✓ Encryption is enabled
- ✓ MFA has been implemented for this remote worker's work account
- ✓ VPN or conditional access is configured
- ✓ Backup for OneDrive has been set up
- ✓ Remote support tool has been installed
- ✓ A security briefing has been completed.

FAQs

1. Should remote employees be issued company laptops?

Yes, the data on a company-issued laptop is far easier to secure and manage than data stored on a personal device (BYOD). Companies should provide employees with company laptops whenever possible, and for occasional remote workers, a BYOD policy can be used.

2. How can businesses keep laptops that are being used at home secure?

Use encryption; implement MFA; set automatic updates; use endpoint protection; create a simple home working guide (password protect your wi-fi; do not allow family members to access the laptop).

3. **Can IT help desk staff manage devices remotely?**

Yes! You can use tools such as Intune or Microsoft Quick Assist to help you troubleshoot/assist users remotely without needing to visit them at their homes.

4. **How often should you replace remote laptops?**

Remote laptops should be replaced every three to four years based on normal usage for a cost of approximately £300-600 per device; plan to replace them in a phased manner.

5. **Is it necessary to monitor employees' devices?**

This is based on the level of risk; you must complete a device health check as well as compliance checks only. You must also be transparent about policy changes and update your Privacy Notice, as well as follow the ICO guidelines concerning monitoring employees remotely.

6. **Are there high costs associated with managing remote machines?**

Microsoft 365 Business Premium has all the security you need in the form of Intune, Encryption, MFA and Defender.

7. **What if someone refuses to use MFA?**

MFA should be a requirement for work content. You should also explain that using MFA secures their own data as well as your work data. Additionally, provide training on how to set up MFA and why it's important.

8. **How do you manage BYOD in an effective way?**

Using MFA is required along with ensuring the mobile device has a separate work profile (Android/iOS) and that you can remotely wipe data (i.e. delete) from the device if it becomes lost. Create a written BYOD policy for your employees.

About This Guide

This guide was created by the **Computer Support Centre** to help UK SMEs (Small and Medium Enterprises) understand how to manage laptops used by remote and hybrid teams in a secure manner. One of the impacts of an increase in remote working throughout the UK is that many employees are accessing the company's systems from home, coffee shops, and client's locations; these types of environments present new types of security and management challenges.

This guide aims to provide practical and uncomplicated ways of managing remote laptops and how to protect the company's data while ensuring staff are working efficiently. Additionally, it covers the primary risks associated with managing remote laptops, examples include lost laptops, weak passwords, outdated software and connecting to unsecured Wi-Fi. As well as highlighting practical controls e.g encryption, remote management software and multi-factor authentication that can be put in place by businesses to meet their obligations under the UK GDPR and reduce potential data breaches.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

 https://computersupportcentre.com

Conclusion

The conclusion summaries the advantages of remote or hybrid working models for contemporary organisations but emphasizes the importance of proper management of company devices (laptops, etc.) to minimize risk (of data loss, cyber attack, etc.) due to lack of controls (lost laptops, weak passwords, operating systems out of date, insecure networks).

Implementing practical management strategies (i.e., encryption, multi-factor authentication, auto-update, endpoint protection, centralised device management) will help to mitigate many of these risks. Along with consistent monitoring through regularly scheduled (to prevent security breaches) and clearly communicated employee policies, using planned replacement cycles will go a long way towards maintaining both security and productivity for the organisation.

While the majority of SME's do not need to use complex management processes to ensure secure laptop management, they must use consistent policies, have the proper tools and service and keep their employees aware through ongoing training to be able to allow flexible working while still providing protection for (the organisation's) data, employees and customers.