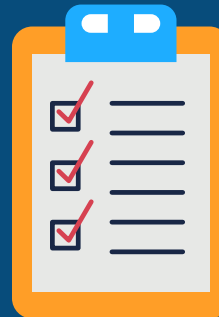


New Device Checklists for Employers & Employees

New Device Checklist: Employer Edition



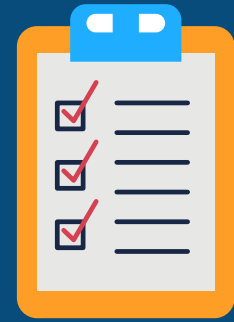
Laptops & Desktops

- ☐ Asset management - Ensure you've recorded;
- ☐ Device make, model & serial number
- ☐ Who is it assigned to & when was it assigned
- ☐ When should it be returned
- ☐ Does the device need to be installed onto your works network?



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE NORTH WEST

How do you ensure new devices are secure from cyber attacks?

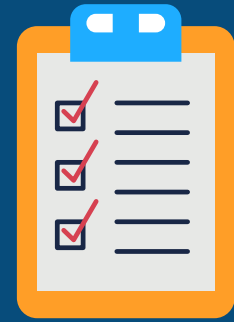


Nearly half of businesses (45%) say that staff in their organisation regularly use their own devices at work. But with most employers still handing over a new laptop or mobile phone to new employees, employers must keep these devices secure from cyber attacks.

Whilst the most common threat to businesses remains phishing attacks - 59% of businesses said they had experienced a phishing attack in the last 12 months, according to the 2023 Cyber Security Breaches Survey. It's important that any device you hand over has some key security barriers in place.

But what barriers, software & hardware should an employer ensure is in place before handing over a new device to an employee?

New Device Checklist for Employers

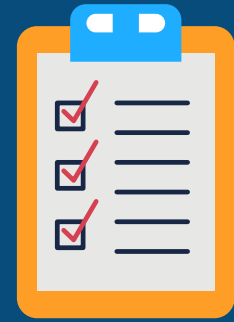


You must ensure the basics are covered with new/current employees who receive a new mobile phone, laptop or tablet.

When sharing guidance on new devices, remember to consider where the device is being used and if your employees are aware of the dangers of cyber security.

- Cyber Security Guidance specific to Laptops/Desktop Computers
- Cyber Security Guidance specific to Mobile Devices (Phones & Tablets)
- Top tips for devices used in the office
- Top tips for devices being used remotely or for staff working from home

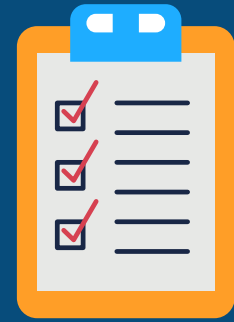
New Device Checklist for Employers



Laptops & Desktops

- ☐ Asset management - Ensure you've recorded;
- ☐ Device make, model & serial number
- ☐ Who is it assigned to & when was it assigned
- ☐ When should it be returned
- ☐ Does the device need to be installed onto your works network?
- ☐ Ensure firewalls and anti-virus software are enabled
- ☐ Ensure operating system updates are installed
- ☐ Ensure application and software updates are installed
- ☐ Make sure that physical and digital files are encrypted
- ☐ Make sure that you backup files daily/weekly
- ☐ Restrict the use and downloading of applications which aren't specific to their job role
- ☐ Ensure the user profiles are setup with the correct permission levels
- ☐ Review plugin device settings to ensure they are secure

New Device Checklist for Employers



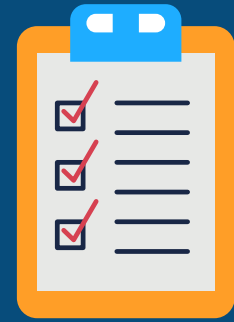
Mobile Devices

- ☐ Ensure that all accounts have Two-Factor Authentication (2FA) enabled
- ☐ Ensure that all accounts are using strong passwords (*remember three random words*)
- ☐ Promote the use of a password manager to keep them secure and encrypted
- ☐ Ensure employees are making use of strong passcodes and Face ID
- ☐ Ensure application updates are set as 'Auto-update'
- ☐ Review all applications - if you want to restrict what employees can download, this should be covered in your company's Device/Security Policy
- ☐ Review the location settings - setup 'Find my iPhone'

Tips in the Office

- ☐ Offline/Cloud backups - ensure that devices are backed up on a regular basis, either daily or weekly.
- ☐ Security Policies - Ensure your staff review all of your company's security policies
- ☐ Cyber Security Policy
- ☐ Password Policy
- ☐ Working From Home Policy
- ☐ Device Usage Policy

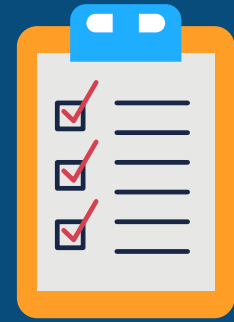
New Device Checklist for Employers



Tips for working from home or remotely

- ☐ Ensure a paid VPN is in use when working remotely
- ☐ Always ensure that you use a unique email address AND password if you sign up for public WiFi
- ☐ Review the web address (URL) of any website you visit/use, ensuring that it is legitimate and where you expect to be
- ☐ Review and ensure each website you visit uses HTTPS by checking for the padlock icon on the left-hand side of the web address (URL)
- ☐ Employees should use a screen privacy protector, webcam cover and secure case for all devices
- ☐ Give your employees regular security awareness training
- ☐ Encourage employees to ask any questions when unsure of any emails/calls/texts they receive
- ☐ Report spam text messages to **7726**
- ☐ Report spam emails to **report@phishing.gov.uk**
- ☐ Report suspicious website to the **NCSC**

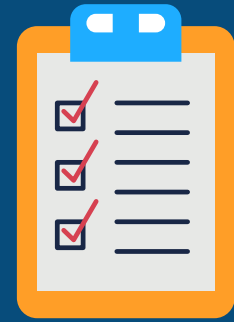
New Device Checklist for Employees



You've been given a new mobile phone, laptop or tablet at work, but what should you do to ensure that device is cyber secure?

- Cyber Security Policies
- Passwords
- External Devices
- Software Updates & Backups
- Personal Accounts
- Data Exposure
- Remote Working

New Device Checklist for Employees



Review your employer's security policies

- ☐ Cyber Security Policy
- ☐ Social Media Policy
- ☐ Working From Home Policy
- ☐ Password Policy

Passwords

- ☐ Ensure you are using Face ID and Passcodes
- ☐ Make sure of a Password Manager
- ☐ Don't forget to use Two-Factor Authentication on all your accounts

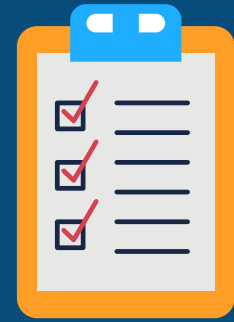
External Devices

- ☐ Do not use unapproved devices
- ☐ Use of any USB or external hard drives should be limited to only ones that your employer has given you
- ☐ Use only the mouse and keyboard that your employer has given you as it's been confirmed to be safe and used with your device

Remote Working

- ☐ Use a VPN when working remotely
- ☐ Be wary of public wi-fi networks - always have your VPN enabled

New Device Checklist for Employees



Software and Applications - Backups & Updates

- ☐ Setup automatic updates for applications, software and your operating system
- ☐ Remember to run regular backups of your data via the cloud or your company's network
- ☐ Only use company-approved applications and software

Personal Accounts

- ☐ Don't use your work email for personal accounts
- ☐ Be careful sharing photos and videos which involve work devices, sensitive data or projects you're working on

Data Exposure

- ☐ Worried your email may have been involved in a data breach? Check [HavelBeenPwned](#)
- ☐ Setup Notify Me alerts on [HavelBeenPwned](#)
- ☐ Don't save any financial details or credit card details
- ☐ Save any work related financial or credit card details within your password manager

Need more support?

Whether you want informal advice, to learn more about your device security or our services and membership. We are happy to help.

Get in touch with our expert team, who can help you on your journey towards cyber resilience.

CALL US: 0161 706 0940

INFO@NWCRC.CO.UK



ARE YOU READY TO PROTECT YOUR BUSINESS?

SMEs in Cheshire can take
advantage of new free membership

nwcrc.co.uk/free-membership

