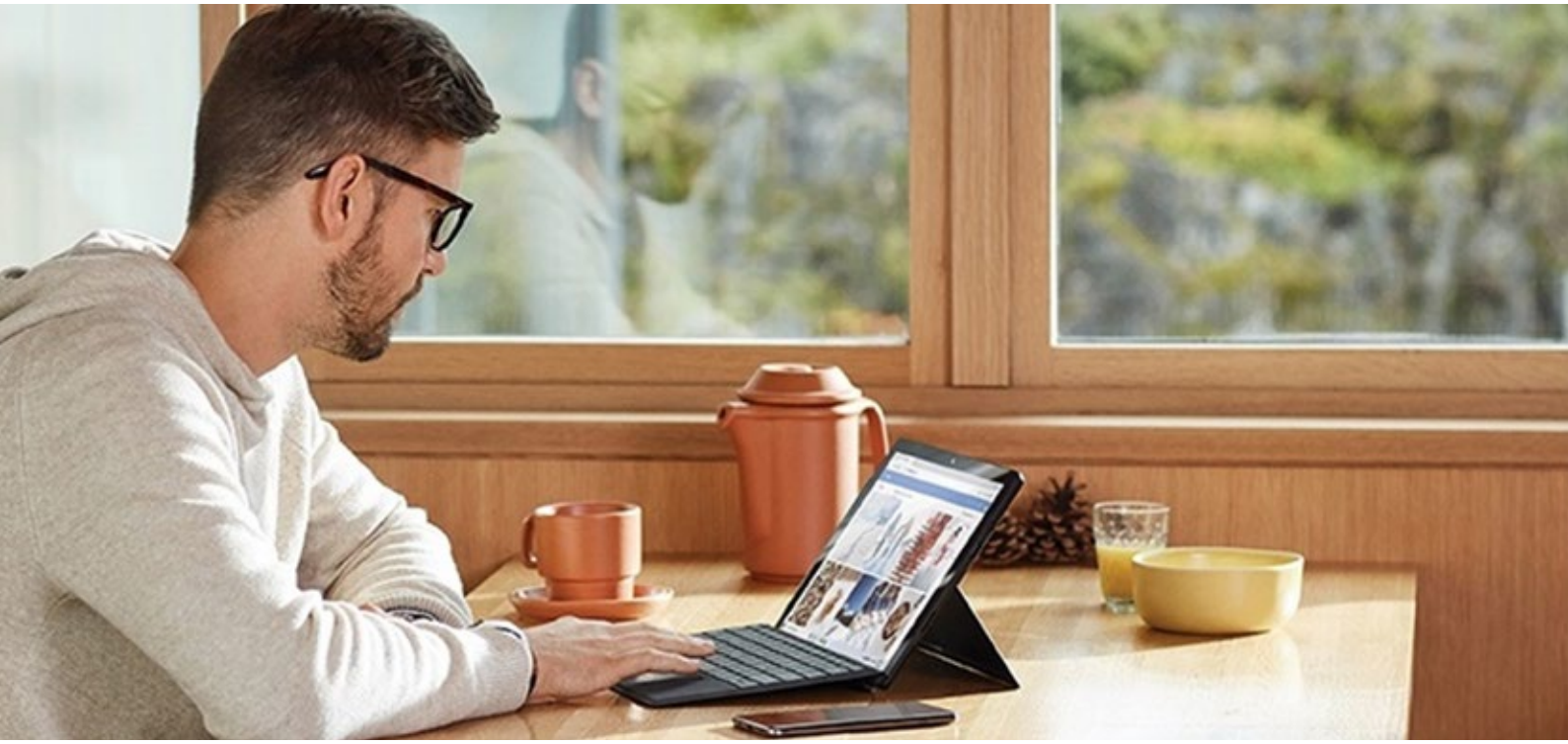


How to optimise remote working with mobile devices

The inherent freedoms that come with remote working can be beneficial to a company's culture and bottom line. It offers greater flexibility in daily routines and removes the confines of a single, and often restrictive, location. This ultimately leads to increased creativity, greater job satisfaction, and greater productivity. However, one of the key advantages of working in a space designated by the company is the infrastructure, which all but guarantees reliable internet connection, purpose-built workspaces, and data storage capabilities.

While working from anywhere has become an increasingly popular option for employees, it can often come without some of the capabilities that are available in a company-operated workspace. Therefore, the success and benefits of remote working depend on the devices employees are using. Giving employees the right tools is essential; however, not all mobile devices are created equal. Unfortunately, it is not as simple as purchasing a standard device; without the right capabilities, a mobile device used for remote working can hinder productivity and affect company outcomes.

There are 10 must-have features of mobile-connected devices for top-performing workers.

1 Enterprise wireless connectivity

Remote working centres around dependable internet access. When employees work remotely, mobile devices cannot rely on physical connections to communicate or send data. Not only are mobile hotspots critical for uninterrupted access on the go, they can also serve as a connectivity backup. Employees working remotely must be able to collaborate seamlessly and, therefore, their mobile devices must have robust wireless connectivity capable of streaming video. This may include continuous connection to cloud-based storage options or wireless/online device-sharing and connection software such as that offered in Microsoft's Surface range, which is revolutionary.

2 Digital storage capabilities

Extra storage space is not a luxury for businesses but a necessity. Tangible hard drives restrict the seamless connectivity that remote workers can enjoy, which is why access to the cloud is essential for any mobile device. Depending on the scale of the enterprise and the number of employees working remotely, storage must also be capable of handling gigabytes, or even terabytes, worth of data without the risk of crashing. Mobile devices such as Microsoft's Surface range provides secured chip-to-cloud that can save files on the physical device while providing backup copies on the cloud which can be accessed by remote colleagues and managers.

3 Video conferencing and screen sharing

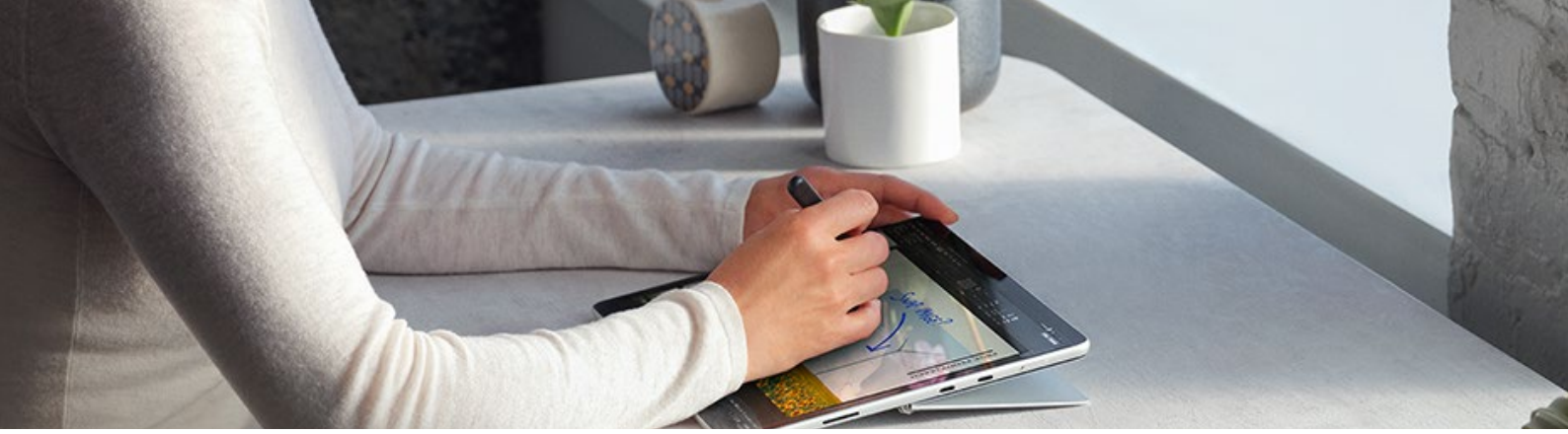
In-built microphones, high-pixel cameras, screen sharing capabilities, and quality speaker systems are essential for remote working and should be included in the features suite for any mobile device. These will provide a seamless connection between employees and improve communication quality regardless of physical distance. Having the ability to share screens seamlessly between colleagues improves collaboration and training experiences.

Screen recording tools are also beneficial. Enhancing employees' ability to connect and communicate will help blur the lines between a conventional office and remote working as well as remove any productivity issues that arise when staff aren't located in the same office.

4 Reliable battery life and streamlined functionality

Remote workers will often multitask or have several applications or resources running on their devices simultaneously. Batteries on remote devices must provide long life when not directly connected to a power source to maximise mobility and flexible remote working conditions. It's therefore important to choose mobile devices that not only boast a long battery life, but also devices that provide 'all day' batteries or 'smart' battery life. These claims often mean that the device can more accurately detect and monitor battery consumption and projected output, which allows them to automatically engage battery saving functions. Functions may include automatically adjusting screen brightness, closing unused or inactive apps and programs, or readjusting the device's sleep function to deactivate the screen quicker.

It's also important to have a device that can predict login habits, application use, forms, and work processes, thereby making accurate predictions that can be tailored to specific needs. For example, devices that use machine learning can provide users with better keyboard predictions, by tracking and processing millions of sentences to understand the relationship between various words better.



5 Up-to-date processing speeds

Apps, programs, and software such as cloud storage are constantly being updated to keep up with digital trends and developing capabilities. Mobile devices that do not use the latest processors may be unable to ensure consistent, reliable operation, which can affect business productivity.

6 Built for modern management

A complex system may be difficult to set up at first and cost not just time, but also money. Make sure that the system is easy to set up and run with minimum effort. The best devices will integrate seamlessly into the business's current infrastructure and help adopt existing processes, keeping workloads low. This may include quick connective abilities to company networks and servers without time-consuming and problematic diagnostics. Remote desktop software is beneficial as IT managers can automate tasks and monitor devices. Microsoft's Remote Desktop client is built into Windows platforms, making it simple to use.

7 Device location tracking

The business should be able to track a mobile device's location to know where its devices are. This is especially important for corporate mobile devices that contain sensitive data. Location tracking as a concept can be challenging because it can be viewed as undermining worker privacy. However, it is extremely useful for emergencies and when an employee loses a device that needs to be recovered.

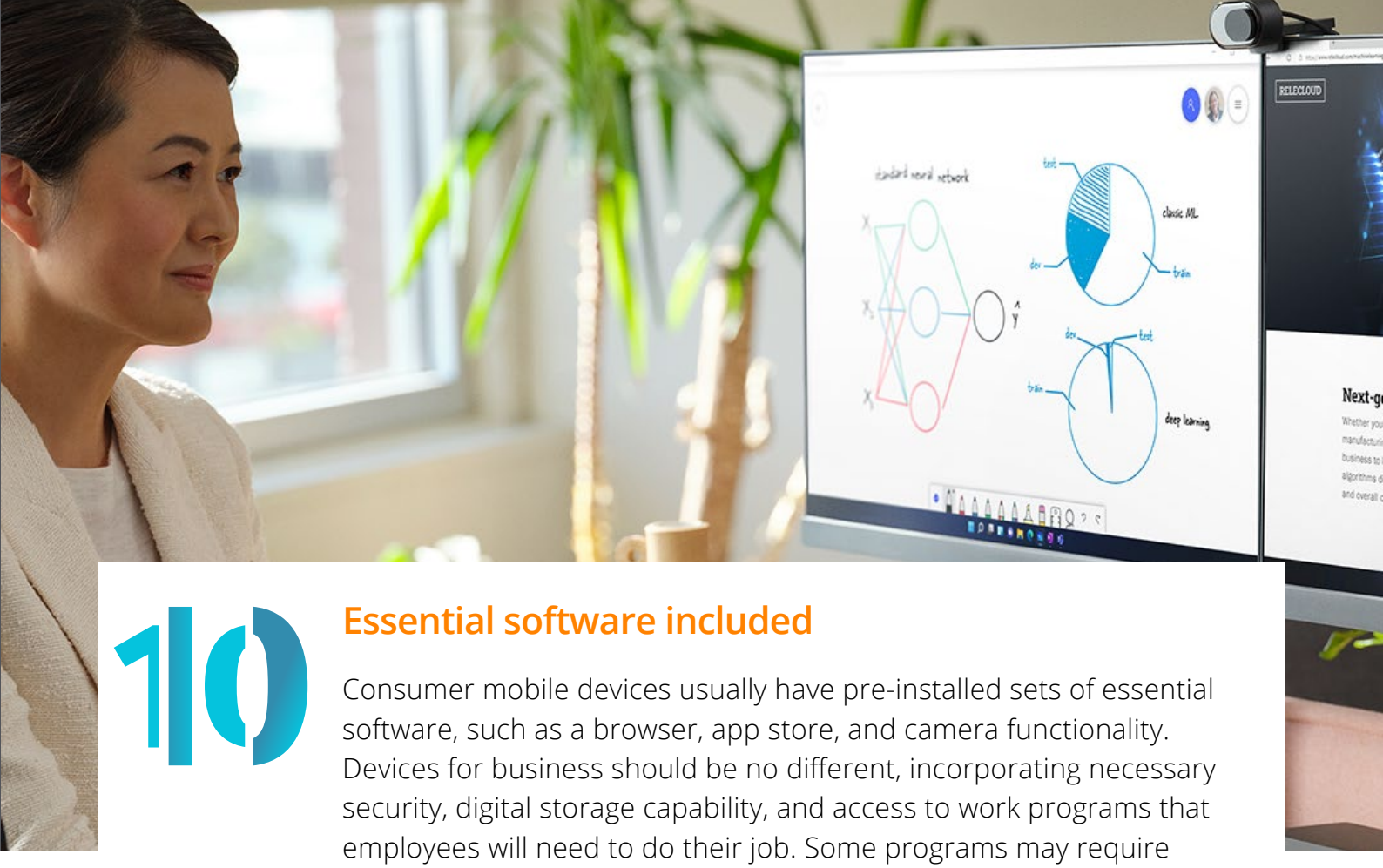
Device analytics and security

Device analytics gives administrators insight into device status, security updates, non-compliant devices, usage, and device health. Reporting tools can help create audit logs that can be streamed to a server to integrate with security incident and event management (SIEM) functions.

Devices must be protected by adequate security measures. Away from the office, at-home devices can be extremely vulnerable. It is important that organisations can remotely protect themselves and the corporate data contained within them from a single management system. The management system should be user friendly and able to easily connect to office firewalls that are necessary for allowing safe software updates. Security features should protect hardware-based data stored on chips and drives as well as cloud-based data and may include data encryption tools, security configuration, and access monitoring. Examples of these include encryption software, password managers, multifactor authentication (MFA), and virtual private networks (VPN).

Team connection apps

Instant messaging (IM) tools are great for keeping distributed remote teams connected. Arguably more efficient than email, IM saves time by allowing messages to appear immediately. It provides colleagues with the contact that working from an office would usually provide.



10

Essential software included

Consumer mobile devices usually have pre-installed sets of essential software, such as a browser, app store, and camera functionality. Devices for business should be no different, incorporating necessary security, digital storage capability, and access to work programs that employees will need to do their job. Some programs may require installing after the fact; however, a set of default programs will help save time in setup. This can be achieved using a mobile device management (MDM) system that also manages and monitors devices.

Having business software and suitable programs to work from home will also prevent the need to download programs that may be incompatible with your business needs to increase the chance of the device being affected by a virus. Surface devices, for example, already provide integrated productivity with Office 365, contain Microsoft 365 chip-to-cloud security, and offer remote management with Windows 11.

Blue Connections works with Microsoft to help businesses maintain productivity while working from anywhere. To learn more about Microsoft's Surface options and how Blue Connections can help your organisation meet its remote working objectives, contact the team today.

Get In Touch:

1800 659 477
enquiries@blueconnections.com.au
www.blueconnections.com.au

BC IT

Microsoft Surface