Managing mobile: should you leave your team members to their own devices

To an increasingly tech-savvy workforce, a wired desktop computer is considered as out-dated as the typewriter. More workers are using the latest smart phones, tablets, portable laptops and electronics to stay informed and connected. As a leader, there are many benefits to letting your team members use their own preferred devices, including:

Flexibility. Mobile devices let employees work outside of traditional office hours and the physical workplace location. For example, remote access software can allow a team member with young children to do some of their work from home – spending less time commuting, more time with their family and still being able to complete the same tasks.

Collaboration. Mobile devices allow people to share information with colleagues and clients more easily. With the touch of a button (or screen), team members can pull up valuable information during team or client meetings.

Productivity. Modern mobile devices include many tools to help your team work more efficiently. Employees may also work more productively on personal devices they are already comfortable using.

Accessibility. A lot can happen after 5:00 p.m. Mobile devices allow key team members to stay easily accessible when their expertise is needed after hours.

However, employees using their own devices for work can also open the door to significant risks and issues, including:

Security fears. Many employees need access to sensitive company and client information as a regular part of their job. If people can get this information from their own technological devices, there is a much greater risk of this data being hacked, lost or otherwise falling into the wrong hands.

Support challenges. If each team member uses a different device, it is harder for your company's IT department to provide updates and support for company applications. Also, not all applications will be fully compatible with all devices.

Distractions. Between social media, games and movies, personal electronics offer many potential distractions.

While challenging, many organizations find it is possible to allow employees the benefits of working from their own tech devices while also taking steps to minimize the risks. Here are some best practices to consider:

Set clear limits. Set clear policies upfront regarding when, where and how personal devices are used to access or share company information. For example, you might allow employees to access only their emails from personal devices, limiting sensitive client information to office network computers.

Stay secure. Any device an employee uses to access sensitive information should be secure. If a team member uses their own tablet, for example, ensure the device has a strong password and up-to-date antivirus software and firewalls.

Educate employees. If access to information on personal devices is restricted for security purposes, take the time to explain the reasons behind the policies to your team. Employees are much more likely to support and follow policies if they have a clear understanding of the reasoning behind them.

Get team input. Since the team is directly affected by office technology policies, it is wise to seek out their opinions before rules and restrictions are formalized. Take an informal survey to gauge the types of devices your staff are interested in using and the work-related information they would like to be able to access on the go. Look for ways to balance your team's preferences with any practical budget and security constraints.

Talk dollars. Employees may expect to receive reimbursement for work-related expenses using personal devices. Have an upfront discussion about which, if any, mobile device costs the company will cover.