Remote Learning and Off-Site Working

In the rush to set up remote learning, districts frantically purchased new devices and technologies. Remote system access has been essential during the pandemic and it is likely that some of the positive changes in working practice will remain.
Schools should ensure that policies and procedures that support mobile working or remote access to systems are reviewed regularly.
Any systems or processes which were implemented as part of the school's Covid response and to support remote learning should be reviewed as time allows, to verify that all necessary security precautions are being taken.
Off-site working means that rather than being connected to the internet via the secure school networks, devices are now attached to home networks with unknown levels of security.
As a minimum, devices should have:

- Supported Operating System
- Antivirus
- Device encryption
- Firewalls
- Web filtering

Incident Management
There is also a need to have robust incident reporting mechanisms for possible security breaches. This process must work for those users who are accessing information away from the main school site.
The incident management plans should be sufficiently flexible to deal with the range of security incidents that could occur, including the loss or compromise of a device.

User Credentials
Remote learning and remote access have led to the transfer and storage of information (or operation of systems) outside of the school infrastructure, frequently over the Internet.
If user credentials (such as usernames and passwords) are stored with a device used for remote working or remote access, and they are shared, lost, or stolen, this is a significant security breach and may also lead to a data breach.
Cyber Essentials asks schools to confirm that passwords are changed if compromised. In order to answer 'yes' to this question, schools need to be aware of what constitutes a **breach**, and be confident that staff members would recognize and report them.
A data breach occurs when information held by an organisation is stolen or accessed without authorisation. This can include destruction, loss, alteration or unauthorised disclosure of school data or lead to further unauthorised access to other school services.

Updating
Ensure users allow updates to run. It is understandable that there will be occasions when updates may be postponed due to the need to use a device at a given time, but staff must not postpone updates repeatedly as this leaves devices vulnerable.
Cyber Essentials requires devices to be kept updated, and in line with NCSC guidance, auto updates should be enabled where possible. Policy and update schedules are no use if users defer them from running continually.

Firewalls

Remote Learning and Off-Site Working

Network firewalls act as the first line of defence against potential cybersecurity vulnerabilities, and schools should have installed them at their network boundary. Software firewalls should also be turned on for teachers, students, and other staff when connecting from home on the device they are using to access school systems.

A number of schools have fallen victim to cyber-attacks after having relaxed firewall rules to support user access to applications and systems.
Firewalls should be enabled to meet Cyber Essentials requirements.
Opening ports in the firewall should only happen when there is a **documented business case** for doing so. A **documented business case** means that the reason for opening a port must be discussed and recorded in the minutes of an audit and risk committee or full governing body meeting. It would also need to be entered into the school risk register and reviewed regularly.

Managing Devices
Understand what your 'standard' device build should be and ensure secure configurations of devices. The National Cyber Security Centre (NCSC) provides advice on Security Controls for End Users.
Staff should use a standard user account to carry out their normal day to day work. A separate administrator account should be used to install and remove software, and other administrative tasks.
Cyber Essentials asks whether users are prevented from downloading or installing unassigned and unapproved applications. In order to answer 'yes', you need to actively prevent this and address it in the relevant policy. This can be achieved through different methods, depending on the Operating System installed. For example, in Windows 10, User Access Controls can be adjusted to only allow installation
through administrator accounts. For specific guidance refer to your Operating System documentation.

Authorised Services and Apps
Teaching staff may have been installing apps and software in an attempt to enrich the learning of their pupils. Many will authorise the app by using their school credentials, whether on purpose or not.
Schools should have a reference list of vetted and approved apps that they can check to see if the app is ok to use. This vetting process should include a Data Protection Impact Assessment (DPIA).
Using this information helps keep the list of approved apps updated and relevant.
Cyber Essentials also requires that as well as a software list, you have a process for approving and provisioning administrative accounts for systems.

Loaned Devices
When you loan a school device, users should sign a loan agreement in addition to the acceptable use agreement.
Returned devices should be checked to ensure they are updated and that they are clean of malware. Any software installed for a specific user should be removed and the device should be returned back to the standard build specification.
Cyber Essentials requires that unnecessary software applications are removed.

Remote Learning and Off-Site Working

Bring Your Own Device (BYOD)
Bring-your-own-device (BYOD) allows staff or pupils to use personal devices to access school networks.
During the pandemic, many schools have been forced to allow the use of personal devices, and pupils in the vast majority of cases, have been expected to connect to school networks with personal devices.
The increase of services such as Microsoft Teams had the effect of encouraging users to install applications on their own smartphones and laptops. In both cases, it's unlikely that personal devices had robust security.
Cyber Essentials requires that devices used to connect to school systems are included in the scope of the submission, and schools must make sure they can manage the security of these devices.

Remote Desktop Protocol (RDP)
Remote Desktop Protocol enables a user of a computer in one location to access a computer somewhere else. This is often used by technicians to support users and to carry out maintenance tasks.
During the pandemic more schools have been enabling remote connections to provide access to apps, software, and files. Some schools have fallen victim to attack after failing to close the RDP port.

- Schools should limit user accounts who can access remote desktop.
- Ensure the latest versions of both server and client software.
- Close or block the RDP port if it isn't required. Alternatively, change the default port to mask the port in use.
- Where possible, rather than using remote connections, utilise cloud services such as OneDrive or Google Drive.

Cloud services
Whilst cloud services prevent the need for remote desktop access, cloud services do need to be correctly configured and users need to have training to understand how to use them securely.
During the pandemic, many schools have increased their use of Microsoft 365 and G Suite, and used tools such as Teams, Zoom, and Google Classroom to offer remote learning.
Cloud platforms are not secure by default and schools are responsible for protecting the data and applications they use.
If employees are using their own personal devices for work purposes, including accessing school data and cloud services which includes email, their devices **will** be in scope for Cyber Essentials.