Schools use a range of technology and may include smartphones, tablets, laptops, desktops and routers, as well as the use of externally hosted systems. Implementation of Cyber Essentials controls can significantly reduce the risk of common but unskilled cyber-attacks.

Services hosted by third parties should be subject to the appropriate due diligence, but most of these are beyond the scope of the Cyber Essentials assessment.

**What is the scope?**

The scope of your network defines what will and won’t be covered by the Cyber Essentials assessment. It is important to identify what is in and what is out of “scope”.

The scope should include the whole school IT infrastructure to achieve the best protection.

**What should the scope include?**

You will be required to identify the actual scope of the system(s) to be evaluated as part of this questionnaire. This includes:

1. **School, Academy or Trust name**

The name of the school, academy or trust will be used on the certificate awarded, so please make sure the name is unique and accurate.

1. **The boundary of the internal network**

Ideally, your scope should be the school network as a whole, because this gives you the most protection and also means you qualify for free cyber insurance\*.

*(\*Your annual budget needs to be less than £20,000,000)*

If part of the network is excluded from the scope it needs to be technically separated, such as by a firewall, which blocks access to the segment which has been included.

1. **The physical location of the school or academy**

Consider whether you have a single or split-site or whether you are assessing a trust with multiple sites.

If you are assessing multiple sites, list all the sites with their basic address.

You should only assess multiple sites on one submission if the procedures and policies are the same in each case.

The document on the official scheme is available at https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure.pdf

**Scope considerations**

When considering what should be in scope, consider the following:

* Do you have a single school site?
* Do you have multiple sites with a shared network or a single network for each? How are they connected?
* Is the pupil/student network different network to the office administration network?
* Do staff work from home?
* Do staff use school owned devices or their own devices for work?
* What cloud services are used (Dropbox, Office 365, Google Drive)?
* Can all of your school and all of your users have Cyber Essentials controls applied?

**Important Points**

1. All devices which connect to the school network and access school data are automatically **in** scope.
2. Devices without internet connectivity are automatically **out of scope**.
3. You cannot exclude devices from scope on the grounds of age or legacy software, if they are connecting to the network.
4. Devices which are managed by your school, that have standard user accounts that connect to the internet for web browsing or opening emails\* are **in** scope.
5. Devices which can be ‘seen’ from the internet, including routers and boundary firewalls are **in** scope.
6. Wireless devices (including wireless access points) are in scope if they can communicate with other devices via the Internet.

**Home Users**

Anyone working more of their time at home than on school sites, and accessing school data including accessing email on a home PC, tablet or mobile phone, is classed as a home worker.

Home workers, and their home internet router, are usually **in** scope if they access any kind of school data.

Firewall controls need to be applied to home routers for home workers and software firewalls on devices must be turned on. Relying on a proxy server is not adequate.

If a Virtual Private Network (VPN) is used to connect to school systems, only the computer accessing the data is in scope and **not** the internet router.

Schools need to ensure that, as well as technical controls, the appropriate policies for remote/home working are in place.

**Bring Your Own Device (BYOD)**

School devices are often managed through centralised administration, ensuring consistency. Assessment of the security controls is usually more straightforward when this is the case.

Devices which are personally owned may be customised, and verifying controls can be more challenging.

In addition to mobile or remote devices owned by the school, user-owned devices which access organisational data or services are **in** scope.

**Mobile devices**

Mobile devices (phones/tablets) belonging to the school, which are used to access the internet, are **in** scope.

Devices belonging to the school, which are used to access school data on the school network or via cloud services (such as email in Office 365 or Gmail) are **in** scope.

A privately owned device with access to school data stored on the school network or via cloud services (such as email in Office 365 or Gmail) is **in** scope.

Privately owned devices connecting to your main school WiFi connection have access to school systems and are **in** scope.

Personally owned devices, using a segregated guest WiFi which prevents the device from accessing the school internal network and data, are **not in scope**.

**Wireless devices**

Wireless devices, including wireless access points, which communicate with other devices via the Internet are **in** scope.

Wireless devices are **not in scope** if there is no communication with other devices over the Internet.

**Cloud Services**

Schools often use cloud services, such as Office 365, GSuite, Dropbox, Microsoft Azure and Amazon Web Services (AWS).

Cyber Essentials scope usually relates to the location you are accessing data from (your home/school), rather than specific cloud hosted services. Cloud services are usually **not in scope**.

Where school systems connect to a cloud provider via a VPN (Virtual Private Network), they may be **in** scope. Please seek advice from your IT Technician.

Software as a Service (SaaS) and Platform as a Service (PaaS) are **not in scope**.

**Remote IT Administration**

If schools are using remote administration services from a third party, it may be difficult for the school to meet the Cyber Essentials requirements directly.

Schools must provide evidence that Cyber Essentials requirements outside their control are met by the service provider, for example that the provider has ISO 27001 certification covering the necessary scope.

**Further Support**

If you have a complex structure, you may need to seek advice from your IT support provider on how you can apply controls and whether this would allow all or part of your system to be included in the scope for Cyber Essentials.