**Cyber Essentials Requirements - Overview**

Version 1.0

**Contents**

[**1.** **Firewalls** 3](#_Toc77166922)

[**2.** **Secure Settings** 4](#_Toc77166923)

[***3.*** **Access Restrictions** 5](#_Toc77166924)

[**4.** **Protection and Prevention** 5](#_Toc77166925)

[***5.*** **Updating Software and Devices** 6](#_Toc77166926)

This document summarises the five key measures required to meet the Cyber Essentials requirements.

# **Firewalls**

Use a firewall to secure your internet connection

If the school router has a boundary firewall function, this should be turned on. Ask your IT provider / technician to do this.

*What is a firewall?*

A firewall is a security device that monitors incoming and outgoing network traffic and permits or restricts data using a set of security rules. A firewall provides a barrier between your internal computer network and traffic from external sources, including the internet. This safeguards against viruses and hackers.

Understand the difference between a personal and a boundary firewall:

* A **personal firewall** can be installed on internet-connected desktops or laptops. Typically, most operating systems come with a built-in personal firewall.
* A **boundary firewall** or **network firewall** is used at the edge of a network in order to protect the network against potential attackers.

Checking the firewall is turned on:

**In Windows**

1. Click Start
2. In the Search for Programs and Files text box, type firewall, and press Enter
3. Click Windows Firewall and check that your computer’s firewall is turned ON

**On an Apple computer**

1. Choose System Preferences from the Apple menu
2. Click Security or Security & Privacy
3. Click the Firewall tab
4. Unlock the pane by clicking the lock in the lower-left corner and enter the administrator username and password
5. Click ‘Turn On Firewall’ or ‘Start’ to enable the firewall

# **Secure Settings**

Choose the most secure settings for your devices and software.

‘Configuration’ is the manner in which components are arranged to make up the computer system.

*Ensuring that you have the most secure settings reduces the likelihood of cyber security incidents.*

Finding the settings on your device can help you turn off functions you don’t need:

* In Windows click on the Start Menu, click the cog icon

and then select Settings within it.

* From the Apple menu, choose System Preferences.

Understand password guidance and security.

Read the NCSC guidance on passwords here: <https://www.ncsc.gov.uk/collection/passwords>

* Update and enforce the password policy
* Understand the restrictions in the security of passwords and know their limitations
* Protect all passwords
* Cope with password overload by considering password managers

What is two-factor authentication?

2FA is an extra layer of security used to make sure that people trying to gain access to a system or account are authorised to do so.

Two factor authentication requires another, second piece of information:

* **Something you know:** this could be a personal identification number (PIN), a password or answers to ‘secret questions’.
* **Something you have:** typically, a text passcode sent to a smartphone.
* **Something you are:** this might include a fingerprint or voice recognition.

# **Access Restrictions**

Control who has access to your data and services.

* Read up on accounts and permissions. Permissions govern what a user or application is allowed to do and access. This ranges from access to systems or application access, to data stored on your phone (like contacts and media file for individuals), through to hardware such as cameras or microphones.
* Understand that any user, program, or process should have only the minimum access necessary to perform the required function. This is the concept of **'least privilege'.**
* Know who has administrative privileges on each machine and for each program or application. Ensure there are two administrators for each system in case there is a need to disable one of these accounts.
* Know what counts as an administrative task and understand who has administrative access and who has responsibility for which tasks.

# **Protection and Prevention**

Protect yourself from viruses and other malware.

* Educate staff on what malware is and how it can get onto devices. Ensure staff recognise issues and report them to appropriate staff promptly.
* Understand that a layered approach to security, involving a combination of preventive measures, is much a much more secure option. Recognise that no one method will prevent all types of attack or issue.
* Ensure installed antivirus applications run in ‘real time’ or are set to auto run. Know who has oversight of the antivirus dashboard to monitor the health of the network.
* When downloading apps use reputable sources such as Google Play and Apple App Store.
* A 'sandbox' is a secure testing environment used to run and test programs safely. Whilst unlikely to be utilised in a school environment, it is useful to understand the terminology.

# **Updating Software and Devices**

Keep your devices and software up to date:

* Over time software will run into problems called bugs. A ‘patch’ is the immediate fix to these problems, and it is essential that updates and patches are applied.
* Verify the operating systems on all of devices is set to ‘Automatic Update’ and ensure there are systems in place for devices which are used irregularly or assigned to users who may be on long term leave.
* Be aware of software you have which is coming to the end of service life/no longer supported. Plan whether the school needs to transition to a new or different product and ensure removal of old legacy software and so called ‘zombie’ (unused) apps.