

# Operating systems, internet browsers and networks supported

## Operating systems

Windows 7 Professional

Windows 7 Enterprise

Windows 7 Ultimate

Windows 8 Professional

Windows 8 Enterprise

Windows 8.1 Professional

Windows 8.1 Enterprise

Windows 10 Professional

Windows 10 Education

Windows 10 Enterprise

Windows Server 2008 Standard

Windows Server 2008 Enterprise

Windows Server 2008 DataCenter

Windows Server 2008R2 Standard

Windows Server 2008R2 Enterprise

Windows Server 2008R2 DataCenter

Windows Server 2012 Standard

Windows Server 2012 DataCenter

Windows Server 2012 R2 Standard

Windows Server 2012 R2 DataCenter

Windows Server 2016 Standard

Windows Server 2016 DataCenter

Windows Server 2019 Standard

Windows Server 2019 DataCenter

Apple OSX – v10.12 or later

Apple iOS – v9 or later

Chrome OS – Shipped with devices from 2013 or later

---

## Internet browsers

Internet Explorer v11– Windows

Microsoft Edge for Windows 10, iOS and Android

Firefox v60 or later – Windows, Apple OSX and Android

Google Chrome v30.0.1599 or later – Windows, Apple OSX and iOS

Google Chrome for Chromebooks– Shipped with devices from 2013 or later

Safari v12.0.3 or later - Apple OSX

Safari shipped with iOS v9 or later – Apple iOS

---

## Networks

Community Connect – v3 or later

Vanilla – Windows Server 2008 or later

Apple OSX – v10.8 or later with Apple Profile Manager

## Android devices

Please be informed that Google have removed support for SSL Interception on Android and on the latest version of Chrome for Android.

Google's policy change will affect all filtering products that support SSL interception to block content in search results.

It is still possible to install the certificate on your Android device but the device browser will no longer trust the certificate.

Users with an sslfilter proxy address will not be able to access search engines or sites that RM have enabled SSL Interception on.

**When access is required for newer Android devices, we recommend using the nosslfilter proxy address. Schools should consider carefully which users are allowed to use school owned Android devices without SSL Interception.**