HTTPS Interception

This system is configured to use HTTPS Interception. For this to work your device may require an additional security certificate to avoid problems with HTTPS sites, in particular those with HSTS or HTTPS certificate pinning.

Please note: You only need to apply the inspection root certificate once. The certificate file is available on this page https://www.wealdofkent.kent.sch.uk/about/portals/staff/wifi-certificate

Microsoft Edge

1. Click the **Download the certificate** button and save the file
2. Open Microsoft Edge and go to the **three dots > Settings**
3. Go to **Privacy, search and services > Security**
4. Go to **Managed certificates**
5. Go to the **Trusted Root Certification Authorities** tab
6. Click **Import**
7. Navigate to your download directory and select the file you downloaded earlier
8. Click **OK**
9. Click **Finished** and close the settings tab
10. Restart Chrome

Chrome (Windows)

1. Click the **Download the certificate** button and save the file
2. Open Google Chrome and go to the **three dots > Settings**
3. Go to **Privacy and Security > Security**
4. Go to **Manage certificates**
5. Go to the **Trusted Root Certification Authorities** tab
6. Click **Import**
7. Navigate to your download directory and select the file you downloaded earlier
8. Click **OK**
9. Click **Finished** and close the settings tab
10. Restart Chrome

Firefox (Windows)

1. Click the **Download the certificate**
2. When prompted select **Trust this CA to identify web sites** and click **OK**
3. Restart Firefox

Safari (OS X)

1. Click the **Download the certificate** button and save the file
2. From the **Finder** menu, go to **Go > Utilities**.
3. Launch the **Keychain Access** application
4. From the **Keychains** panel, click **System**
5. From the **Category** panel, click **Certificates**
6. Create a new keychain by clicking the **[+]** at the bottom of the Keychain Access window
7. Navigate to your download directory and select the certificate file
8. Click **Open**
9. If prompted, enter your MAC password and click **Modify Keychain Access**
10. Double-click the relevant certificate in the list
11. Expand the **Trust** section
12. In the **When using this certificate** drop-down, select **Always Trust**
13. Close the certificate window
14. When prompted, enter your MAC password to confirm the changes and click **Update Settings**
15. Close the **Keychain Access** window

iPad, iPhone, iPod, iOS (Safari)

1. Click the **Download the certificate** button
2. In the settings app go to **VPN & Device Management**
3. Select **Guardian HTTPS Inspection CA** under downloaded profile
4. Press **Install**
5. If prompted, enter or configure your password to confirm
6. Navigate to **Settings > General > About > Certificate Trust Settings** and enable **Full Trust for Root certificates**

Android (Chrome)

1. Click the **Download the certificate** button
2. When prompted, enter a name of your choice for the certificate
3. Click **OK**
4. If prompted, enter or configure your password to confirm
5. If prompted, enter a certificate name
6. If prompted, from the **Credentials use** drop-down select **VPN and apps**
7. Click OK
8. To confirm certificate installation was successful, navigate to **Settings > Trusted credentials**
9. Select the **User** tab to view user installed certificates

Chromebook, ChromeOS

1. Click the **Download the certificate** button and save the file
2. Open Google Chrome and go to the **three dots > Settings**
3. Go to **Privacy and Security > Security**
4. Go to **Manage certificates**
5. Go to **Authorities** and click **Import...**
6. Navigate to your download directory and select the file you downloaded earlier
7. Select **Trust this certificate for identifying websites**
8. Click **OK**
9. Click **Finished** and close the settings tab