Hardware & Software Support and Configuration

Collin May | Last updated 2022-04-01

The following information should help CareLearners figure out what hardware and software they can use, and how the software should be configured. Keep in mind that technology changes quickly. See Appendix B of the latest Core Platform Admin Guide for additional detail.

Supported Hardware

- You will need some sort of computing device (a phone, a tablet, or a personal computer). Personal computers have the most support and are recommended.
- Tablets are supported in landscape mode only, and landscape is recommended for phones as well.
- Devices need a screen resolution of at least 1024x768.
- CareLearn is a web-based application, so you will need to be connected to the internet while using it. Although the SumTotal app for mobile devices does provide some support for offline usage, we do not support its use. We recommend a wired connection rather than Wi-Fi, although both are supported.

Supported Mobile Devices

The following devices and operating systems can make use of the SumTotal mobile app.

- iPhone running iOS (versions 14-15)
- iPad running iOS (versions 14-15)
- Android phones or tablets (Versions 9-12)

Supported Browsers

The following browsers are supported.

- Google Chrome (version 78 or later)
- Microsoft Edge (Chromium post-2020, version 42 or later)
- Mozilla Firefox (version 70 or later)
- Apple Safari (version 12.x & 13.x)

Browser Configurations

If you have trouble configuring your web browser please try to find someone locally to help you. If you have no one to support you, please email carelearnsupport@dshs.wa.gov.

For All Browsers

- Configure your **Internet Options** to include the following as **Trusted Sites**:
    - Next to the **Start** button at the bottom left of your task bar / screen there should be a search box or a search icon (magnifying glass). Search for "**Internet Options**."

    - Click the **Internet options** app that shows in your search results.
    - Click the **Security** Tab.
    - Click **Local Intranet**, and then click the **Sites** button.
    - Select the following options:
        - **Include all local (intranet) sites not listed in other zones**
        - **Include all sites that bypass the proxy server**
        - **Include all networks paths (UNCs)**
    - Click **OK**.
    - Click **Trusted Sites**, and then click the **Sites** button.
    - Temporarily UN-Check **Require Server Verification** if it is checked.
    - In the **Add this website to the zone** box enter each of the following one at a time and click the **Add** button (note that several begin with an asterisk; include it).
        - https://sowa.sumtotal.host
        - *.elsevierperformancemanager.com
        - *.webinservice.com
        - *.educode.com
        - *.collegeofdirectsupport.com
    - RE-Check **Require Server Verification** if it was checked.
    - Click **Close**.
    - Click the **OK** button.
- Enable cookies (should be enabled based on the first configuration above).
- Allow pop-ups (see browser-specific instructions below).

Chrome

- Click the **Chrome** menu on the browser toolbar.
- Select **Settings**.
- At the bottom of the page, click **Advanced**.
- In the **Privacy and security** section, click **Site Settings**.
- Under **Additional permissions**, configure the following:
    - Cookies and other site data – Allow all
    - JavaScript - Allowed
    - Flash – Ask first
    - Images – Show all
    - Plug-ins – Run automatically
    - Pop-ups and redirects – Allowed

Edge

- Click the **Ellipsis** in the toolbar and select **Settings**.
- Click the **View advanced settings** button.
    - Turn **Block pop-ups** off

Firefox

- Click **Options**
- Under the **Content** tab:
    - UN-check **Block Pop-Up windows**.
    - Check **Accept cookies from sites**.
- Click the Security tab
    - Check **Warn me when sites try to install add-ones**.

Safari

- Click the **Options** button on the browser toolbar.
- Click **Preferences**.
- Ensure that you configure the following tabs. When finished, close the window.
    - Under **Web Content**:
        - Check **Enable plug-ins**
        - Check **Enable Java**
        - Check **Enable JavaScript**
        - Uncheck **Block pop-up windows**
    - Check **Ask before ending a non-secure form to a secure website**
    - Under **Privacy**
        - Under **Block cookies**, select **From third parties and advertisers**.
    - Under **Limit websites access to location services**, select **Prompt for each Website Once**