Word Prediction Standard and Special Access	Windows, macOS, ChromeOS, and iPadOS

*iPadOS: It is highly recommended to use an external mouse.

III. Technology Setup

A. Network Connectivity

All student testing devices should have access to the internet and be able to access the server using HTTP/HTTPS protocols on ports 80 and 443.

Allow the following sites on ports 80 and 443 in content filtering proxies or other locally used proxy software.

- `https://mcas.cognia.org`
- `https://mcas-training.cognia.org`
- `https://mcas-practicetest.cognia.org`
- `fonts.googleapis.com/`
- `themes.googleusercontent.com/`
- `googleusercontent.com/`
- `https://cognito-identity.us-west-2.amazonaws.com`
- `https://cognito-identity.us-east-1.amazonaws.com`
- `https://eventsapi.emetric.net/maprod/router`
- `app.getsentry.com`
- `dc.services.visualstudio.com`
- `az416426.vo.msecnd.net`
- `speech.beta.cowriter.dev`
- `wss://*.cowriter.dev`
- `https://ws.cowriter.dev/`
- `https://www.google.com/speech-api`

Note for ChromeOS: If your school/district restricts student browsing using the built-in URL blocking policies within the Google Admin Console (separate from the network firewall or content filters), you must format the CoWriter domain exception exactly as follows:

- `cowriter.dev`

If you are working with sandboxing applications, complete one of the following steps while installing the kiosk, and contact the MCAS Service Center with questions:

- Choose a network folder location for local caching.
- Make sure the default location, such as **C:\Users\user\AppData\Local\eMetric (%localappdata%/emetric)**, and its contents are not deleted by the sandboxing applications.

Note: Student testing data, including encrypted responses, will be saved to the indicated location only if the network connection or internet connection is lost during the test. Students will be able to continue testing without interruption, but their testing data will be saved in the indicated folder.

Note about OneDrive:
OneDrive notifications may interfere with the kiosk and student test taking experience. If OneDrive attempts to steal the screen's focus during testing, the kiosk will display a white screen. The student will then have to click anywhere on the white screen to regain focus in the kiosk; once clicked they will be able to resume testing where they left off. To prevent this, schools should use one of the following approaches:

- If OneDrive is not needed or used on student devices, schools are recommended to disable OneDrive during student testing.
- If OneDrive cannot be disabled, please take necessary steps to prevent any administrative actions, including file sharing or synchronization and administration updates to OneDrive settings, that would trigger a OneDrive notification during student testing.

B. Bandwidth

The ability of a school's network to support a given number of online testers is a function of the available bandwidth between the student's test device and the data center serving the test content, the number of students who will be downloading tests, and the size of the test content. The Site Readiness tool's Connection Capacity Test will measure the bandwidth between a student's test device and the data center and determine the number of tests that can be downloaded at the school simultaneously. Use the results of this test to gauge the impact your bandwidth will have on student testing.

Schools with low internet bandwidth (i.e., an internet download speed of less than 1.5 Mbps or an internet upload speed of less than 256 Kbps) should stagger student start times by 1–2 minutes to reduce the likelihood of interruptions.

C. Thin-Client Environments

When using thin-client environments, such as Terminal Services, Citrix, or LTSP, make sure that there is enough memory, CPU, and bandwidth on the server to accommodate multiple student test sessions. The kiosk requires a minimum of 80 MB of memory per client session and performance can vary depending on the size and type of the test. Allowing multiple sessions on an improperly sized thin-client environment will result in poor performance.

Additionally, schools using thin-clients need to be cautious when there is 1 GB or less of physical memory on the student testing device. In this case, a local installation is strongly recommended. As a rule, if you can use the Chrome browser to access web-based email or web-based streaming services on all student testing devices simultaneously, then testing should go well.

In thin-client environments, the accounts students use to log in to the student testing devices (not the MCAS test login) must be unique for each student. Also, each account must have its own dedicated user profile.

For assistance, contact the MCAS Service Center at mcas@cognia.org or 800-737-5103.

D. Monitor Settings

Ensure that all monitors used for testing are set to the default color settings. If a student will use the zoom in/out tool, review the recommended screen resolutions in Table 4 below:

Table 4. Monitor Settings

Required Zoom Level for Student	Recommended Screen Resolution
100% (No Zoom)	1024 x 768 (or Higher)
150%	1920 x 1080 (or Higher)
200%	1920 x 1080 (or Higher)
300%	1920 x 1080 (or Higher)

Note: Students should use the screen resolution that is most comfortable for them; the resolutions listed are recommendations only. The student or test administrator may set the zoom level within the MCAS Student Kiosk when the student logs in at the time of testing.

IV. MCAS Student Kiosk Installation

A. ChromeOS App Installation

Managed Chromebooks

These instructions are for technology coordinators who have access to the Chromebook device management console to administer and manage their Chromebook devices.

Note: For ease of copying configuration URLs into the Google Management Console, a Quick Copy Guide is available for download on the MCAS Resource Center.

Step 1: Set up your school technology.

Review section II: Technology Guidelines and section III: Technology Setup in detail. If the MCAS Web App for ChromeOS was previously installed for the 2025–26 school year, confirm that all previous configuration requirements remain in place and complete steps 10–13 in the ChromeOS instructions, which outline new steps to disable Chrome Accessibility features.