CMS Technology System Requirements

Enabling the delivery of rich digital resources to Charlotte-Mecklenburg Schools (CMS) students and teachers is a priority for CMS Technology Services. CMS strongly prefers the purchase of digital content, assessment tools, and applications which conform to the technical standards adopted by the division of Technology Services. The aim of this is to ease access for both teachers and students to learning resources and standardize the way in which CMS integrates with content and service providers. Included below are descriptions of concerns that CMS frequently encounters when integrating with education technology vendors. All digital resources must align with CMS technology standards. This means it must not be in conflict with district technology initiatives, projects and positions and must be fully operable on existing equipment within the district which is described below.

Hardware

Workstations

CMS maintains a set of technology standards which define the workstation hardware and software specifications. The technology specifications will change with time, as technology changes. For the purposes of this proposal, CMS technology PC standards currently call for a minimum specification for new equipment as follows:

Desktops

Make: Lenovo
Model: M70g Tiny
Processor: Minimum Intel Core i-3
Storage: Minimum 256Gb SSD
Memory: Minimum 8 GB memory
Network: Gigabit Ethernet interface card

Laptops

Make: Lenovo
Model

- Thinkpad L14 Gen 4

Processor: Minimum Intel Core i-3 3.4 GHz Processor
Storage: Minimum 128Gb SSD
Memory: Minimum 8 GB memory
Network: Gigabit Ethernet interface card
Peripherals (may include, but not limited to)

- Integrated camera & microphone
- 2 USB ports
- HDMI port
- Wireless 802.11 ac compatible

Make: Lenovo
Model

- Thinkpad X1 Yoga

Processor: Minimum Intel Core i-5
Storage: Minimum 256Gb SSD
Memory: Minimum 16 GB memory
Network: Gigabit Ethernet interface card
Peripherals (may include, but not limited to)

- Integrated camera & microphone
- 3 USB ports
- HDMI port
- Wireless 802.11 ac compatible

Chromebooks

Chromebooks devices are provided to CMS students in Grade 3 through 12.

Make: Lenovo
Model: 300e Yoga Gen 4 11.6”

Tablets

Apple iPads are provided to CMS students in Grades K through 2.

Hardware:

- Apple iPad generation 10 and above
- Apple iPad Air 11” and 13”
- Apple iPad Pro 11” and 13”

OS:

- iOS version 18 or above
- iPadOS version 18 or above

IoT (Internet of Things) Devices

Some solutions require the use of IoT devices to function. CMS separates IoT device traffic to a separate, encapsulated, dedicated network. Wireless access to the IoT network is enabled for approved devices and involves MAC filtering. Wired access to the IoT network is only enabled if a firewall appliance is purchased separately with approval from Technology Services. The cost of the firewall appliance must be covered by the requester and should be factored when considering procurement of IoT solutions. Note that while a vendor may not label a device IoT, it is up to CMS to determine if it qualifies for IoT status.

Software

Operating Systems

Windows 10 Education/Enterprise (OS)
Windows Server 2022
WIndows SQL Server 2022
Office 365/Microsoft Office

Internet Browsers

- Google Chrome* With the latest whole number version update
- Safari
- Microsoft Edge

Google Chrome is the preferred browser when accessing all digital resources. Digital resources must deliver full functionality when accessed using Google Chrome. Our Chrome browser is configured to automatically update within 10 days of a new release and services should adhere to the requirements within the last two whole number OS versions.

Browser Plug-In Software

CMS limits the use of third-party plugin software. Adobe Flash and Oracle Java are not supported on student devices. Google Extensions require individual approval and allowlisting before they can be used on student devices.

Software Permissions

CMS employees do not have administrative rights on their individual computers. Users are not members of domain or local administrator groups in Windows. Administrative permissions will be removed from Mac devices during the 24-25 school year. Installation of software, drivers, peripherals, etc. requires the assistance of a CMS Technology Support Specialist.

Mobile Device Management

CMS utilizes MDM software for remote device management of tablets and some other compatible devices. Digital resources must be capable of deployment using JAMF MDM software. Unmanaged devices require installation of digital resources individually on each device.

Learning Management System (LMS)

CMS uses Canvas as a Learning Management System (LMS). Digital resources can be delivered to students within the context of courses in Canvas through the use of Learning Tools Interoperability (LTI1.3 and LTI Advantage), Common Cartridge (CC), Thin Common Cartridge (TCC), and Question & Test Interoperability (QTI 3 and Assessment). In addition to accessing digital resources through Canvas by leveraging these standards, students and teachers can be rostered into the vendor platform using LTI 1.3.

Edtech software vendors' Canvas integrations vary greatly. If you intend to integrate with our Canvas instance, please provide documentation on how your digital resource will be implemented/installed in Canvas, including any rostering that is required of the tool. We cannot guarantee support for integrations based on the vendor's word alone.

CMS additionally utilizes blueprinting to deploy curricular content to teachers. If you intend to use the Canvas blueprint functionality with your digital resource/tool, you must verify with the vendor that this will work. Many external tools do not blueprint or require additional setup by the teacher.

PowerSchool Integration

CMS uses PowerSchool Student Information System. Digital Resources that leverage integration with PowerSchool must rely on the PowerSchool API to do so. Data Export Manager (DEM), Direct Database Export (DDE) and Direct Database Access (DDA) are not acceptable methods of integrating digital resource data into PowerSchool. Integration of vendor-supplied plug-ins is restricted to read-only data access out of PowerSchool and requires prior approval of the CMS PowerSchool team. Plug-ins must use PowerQueries or read-only API access. Plug-ins that incorporate page content are not permitted.

Video Streaming

CMS restricts access to many video streaming services (e.g. Vimeo). If digital resources utilize video content for instruction, training or otherwise, the video content must be hosted on an CMS-approved third-party streaming service or the content must be hosted privately by the software vendor so that filtering rules can be enabled to allow access by CMS students.

Content Filtering

CMS filters Internet content on CMS-supplied student devices. Vendors must identify all domains hosting online content necessary for full functionality of the digital resource. The rules necessary to enable access to this content must be approved by Technology Services.

Video Conferencing

CMS staff and students use the Microsoft Teams video conferencing platform. The use of any other video conferencing service in association with teaching and learning must be approved through academics and technology services.

Email

Student Email

Digital resources that depend on email for communication with students require approval through Technology Services. By default, domains other than cms.k12.nc.us are blocked from sending email to students and for students to send out to non-CMS recipients.

Staff Email
CMS imposes no technical restrictions on staff email.

DMARC
CMS prefers vendors to employ DMARC to facilitate reliable delivery of legitimate email to students and staff.

Data Security

Ownership
All data provided by, collected on behalf of and stored in relation to a software subscription or service contract should be considered to be owned by and in control of Charlotte Mecklenburg Schools. This is a basic requirement of FERPA. Student data may not be sold, licensed or shared without written consent of CMS leadership.

Locality
Data processed and stored in connection with the delivery of the digital service should be physically located only within the borders of the United States of America. Any exception to this should be identified by the vendor so that CMS Technology Services can evaluate whether or not appropriate safeguards are in force within the country where the data might reside.

PCI DSS Compliance
Digital resources that collect and process credit card information require separate approval of the **CMS Finance department**. Any digital resource that collects or processes such information should offer proof of PCI DSS (Payment Card Industry Data Security Standard) compliance. Vendors should also be prepared to demonstrate compliance of any system or component used to process, store, or transmit cardholder data that is operated by the vendor as part of its service. Similarly, the vendor should be prepared to demonstrate the compliance of any third party it has sub-contracted as part of the service offering. As evidence of compliance, the vendor shall provide upon request a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor).

Data Encryption
Digital resources that collect and process CMS data should encrypt CMS data, both at rest and in transit, in a manner consistent with the strongest encryption standard that is commercially reasonable at the time of the agreement.

Data Deletion
Digital resource vendors should describe their ability to delete CMS data upon demand. Data deletion requests extend to electronic backup files as well as physical records. CMS expects a vendor to be able to delete all CMS data within 30 days of receiving such a request.

Data Re-Use
Vendors will agree that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the service contract. CMS data shall not be distributed, repurposed or shared across other applications, environments, or business units of the vendor. The vendor further agrees that no CMS data of any kind shall be revealed, transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis and as specifically agreed to in writing by CMS.

Data Breach
No content

Personally Identifiable Information
Student personally identifiable information (PII) is protected under federal and state laws as well as CMS board policy. Digital resource vendors should describe, in detail, the PII that is collected from students (and staff). Data that CMS has identified as PII data can be found in this document. CMS PII Data.

Other Concerns

Accessibility
ADA and Section 504 requires all digital materials to be fully accessible to students with disabilities. WCAG 2.0 AA (Web Content Accessibility Guidelines) is the standard. Digital resources should be fully accessible and conform to WCAG 2.0 AA. Vendors should provide a Voluntary Product Accessibility Template (VPAT) and it should be submitted with the proposal.

Reporting
No requirements exist presently for Reporting.

Support
Vendors should describe in detail the method and manner by which CMS students, teachers and staff seek and receive both technical and functional support for the contracted digital resource. Points of contact should be identified by both parties. Escalation protocols should be defined. CMS business owners should work with Technology Services to advise the Technology Services help desk on identification of the issue, gathering the necessary details, and routing the CMS MySupport ticket to the appropriate business owner support group. CMS business owners will identify primary points of contact for software support and will use CMS MySupport for support/service requests.

Learning Object Repository (LOR)
No requirements exist presently for LOR.

Authentication
Digital resources requiring users to authenticate should be capable of allowing students, teachers and staff to authenticate via one or more of the following authentication services (in order of precedence):

- ClassLink - CMS uses ClassLink to make resources accessible to students. ClassLink provides secure access and MFA capabilities for students.
- ADFS (using SAML 2.0) - Typically, resources that are authenticated using ADFS are targeted at staff, since students rarely use Active Directory accounts for authentication.
- Canvas LTI (launch request) - LTI works on the basis of a trust relationship between Canvas and the digital resource which is established by way of a key and secret. In LTI, the user is authenticated by the LMS (Canvas) and then passed to a digital resource by way of a signed launch message. (https://www.imsglobal.org/learning-tools-interoperability-sso-mechanism)

Authorization
Vendors should describe how authorization is configured in the digital resource. Typically, authorization falls into one of two methods; group-based or role-based security. With group-based security, end users obtain permissions by virtue of coalescing the permissions for the group(s) to which he/she belongs. With role-based security, roles are assigned permissions and users inherit those permissions depending on the role under

which they're acting during any given session. Additionally, the digital resource should allow for the automatic management of these authorizations through the use of an import mechanism or integration.

Rostering

Digital resources should provide for automated student, teacher and staff rostering via one of the following services:

- DPI (if SEA-sponsored)
- ClassLink (OneRoster)
- Canvas (via LTI 1.3) - please provide documentation and notice if there needs to be additional rostering through ClassLink with Canvas rostering.
- CMS standard rostering solution - Specifications available on request. This solution only allows for nightly full rosters, not filtered files or differential updates. Files are only transmitted via SFTP. Distinction should be made whether the files will be pushed by CMS or pulled by the vendor (PUT vs GET).
- Microsoft Excel upload - managed by the individual school administrator or other contact. This is not ideal and should only be used if a small number of users are rostered into the software or as a last resort.

Video and Sound Capture

Digital resources that collect and process sound (e.g. student dictation) or video should be compatible with the inherent limitations of low-resolution cameras in Chromebooks or other devices as well as the intrusion of ambient noise in classroom environments that may distort or impede sound capture.

Wireless Networking/Bluetooth

Digital resources that rely on peripherals to connect to a laptop, desktop or Chromebook wirelessly should indicate the minimum wireless networking specifications and be compatible with the baseline specification for laptops, desktops, Chromebooks and tablets in use at CMS. If dongles or outboard peripheral devices are required to facilitate wireless communication between the device and the computer the cost, maintenance, loss, and compatibility of the peripherals should be taken into account.

Adhoc/P2P (peer-to-peer) networking is disabled on Chromebooks. Solutions that require P2P networking will not be usable with a student device.

Social Networking

Digital resources should identify whether or not there are social networking aspects to the digital resource. Examples include message boards, chat features, video conferencing, voice communication, other forms of interaction or communication between the student and anyone other than the student's teacher. Of special concern are social networking features that would allow student work or personal information to be published such that anyone outside the CMS organization could view, comment, rate the work or make contact with the student.

Parental Review and Corrections

Vendors should describe how the digital resource allows parents the ability to inspect and correct their student's information. This right is provided for by FERPA.

Exhibit A - Examples of Student Data

Information in the student's educational record or electronic mail.
First and last name.
Home address of the student or student’s family.
Telephone number.
Electronic mail address.
Other information that allows physical or online contact.
Discipline records.
Test results.
Special education data.
Juvenile dependency records.
Grades.
Evaluations.
Criminal records.
Medical records.
Health records.
Social Security number.
Biometric information.
Disabilities.
Socioeconomic information.
Food purchases.
Political affiliations.
Religious information.
Text messages.
Documents.
Student identifiers.
Search activity
Photos.
Voice recordings.
Geolocation information[HAW1]
Attendance.
Promotion.[HAW2]
Name of the student’s parent or other family members.
Personal identifier, such as the student’s Social Security number or unique student identifier.
Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name.

Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

Versions

Version	Date	Comments
1.1	07/13/2021	Updated for SY 2021-22
1.2	07/13/2021-?	Suggested Edits
1.3	02/01/2023	Updated for SY 2022-23
1.4	08/27/2024	Added IoT section