Cache County School District

Policy Series 4000: Curriculum, Instruction, Assessment

Policy No. 4625 P1

Software Approval

This document sets forth the official workflow for submitting and evaluating requests for digital tools and services—including software, websites, applications, and Software-as-a-Service (SaaS) platforms—that require user accounts, data sharing, integration with district systems, or instructional implementation. The purpose is to create a transparent and secure vetting process for all resources intended for use at the classroom, school, or district level.

A request will result in one of two outcomes:

1) **Approved:** The resource is determined to be fully compliant with district security protocols and data privacy policies, including other requirements, and is permitted for use on district devices and/or with employee or student data.
2) **Denied:** The resource fails to meet the required standards and is not permitted to be accessed, installed, or otherwise utilized on any district device or network.

The evaluation process focuses on three primary areas: the privacy of student and staff data, alignment with district curriculum and teaching standards, and overall data security.

Only current staff are permitted to submit a request for approval. No solution shall be purchased, installed, or have any protected data uploaded or shared until formal approval has been obtained.

Teaching and Learning Review

1) All software requests will undergo a curriculum review by the designated subject-area expert, as determined by the executive director of teaching and learning.
    a) The subject-area expert will review the request for standards and district alignment, and determine:
        i) if current district software, websites, or programs are an adequate solution, or if the requested software brings something that is not currently provided; and
        ii) if the requested software aligns with district screen-time standards.
2) Software requests that do not involve teaching standards, such as business applications and productivity tools, may be noted as non-applicable and bypass the teaching and learning review.
3) If subject-area experts determine that the requested software meets a documented need that an existing approved solution does not adequately meet, the request receives teaching and learning approval and is forwarded to the security officer for review. Otherwise, the request is denied, and the requester is informed of the decision.

Data Security Review

The following steps are used to evaluate and approve new software for district use, ensuring it meets our security and compatibility standards:

1) verify system compatibility by confirming that the software's system requirements, including operating systems and hardware specifications, are compatible with district devices intended for its approved use;
2) assess website and vendor credibility by using security and transparency tools, such as Cisco Talos and the Google Transparency Report, to validate the legitimacy and security of the vendor's website and the download source;
3) confirm software maintenance, ensuring the software is actively maintained and receives regular security patches and updates from the developer;
4) validate software sources, verifying that the software is downloaded directly from the official manufacturer's website to prevent the installation of third-party modifications or bundled malware; and
5) check for vulnerabilities by researching any known vulnerabilities or recent compromises of the software or its manufacturer using the NVD (National Vulnerability Database).

Upon the security officer's review and approval, the request will be forwarded to the student data privacy manager. Any denial will be recorded and shared with the requester.

Data and application security is fluid; the district reserves the right to revoke data security approval for any application at any time based on newly found vulnerabilities or other system incompatibilities determined by the security officer. If this occurs, the following process will be followed:

1) notify staff of the pending revocation of software.
2) work with the student data privacy manager to remove the affected software from the district's approved list of applications.
3) work with district technology teams to remove software installations.

Student and/or Staff Data Privacy Review

1) **Request involves student data**
    a) Consultations with curriculum specialists are sought if a district-approved alternative exists.
    b) Terms of service and privacy policy are reviewed.
        i) If necessary, district legal counsel will review any items in question in the privacy policy to ensure the district's best interests are served.
        ii) A vendor may be asked to adjust wording to meet district standards and requirements.
    c) If an existing DPA is in place with another LEA, an Exhibit E is signed, allowing the district to adhere to the terms already established.
    d) If no DPA is available, the vendor is contacted, and a DPA is shared with them. The vendor is responsible for completing the DPA. Once the DPA is complete, it

is sent to our business administrator for signatures and then uploaded to SDPC (the statewide database).
    i) If a vendor refuses to sign or is unresponsive, the request is denied.
    ii) Once a DPA is completed, the software meets data privacy approval.
2) **Request involves staff data**
    a) Verify that data sharing complies with local and federal laws.
    b) Verify that data sharing complies with the district privacy plan.
    c) Determine if an MOU or other formal data agreement is appropriate; consult with legal counsel if necessary.
    d) If needed, bring the request to the full data privacy committee.
3) **Request involves neither staff nor student data**
    a) Student and staff review may be bypassed and noted as non-applicable for this portion of the process.

Decision

1) **Approval**
    a) Software becomes officially approved and may be used or installed if/when:
        i) the software does not involve student data, final approval will be based on approval from the teaching and learning and data security reviews; and
        ii) software involving student and/or staff data receives approval from all three review processes.
            (1) Portions of the reviews that are bypassed as non-applicable are deemed to have passed that portion of the process.
2) **Denial**
    a) If any of the three reviews find that the software does not meet district standards or requirements, the request will be denied.
    b) The district reserves the right to deny any request regardless of meeting other requirements due to:
        i) The request is not in the best interest of the district, determined by the combined assessment of the student data privacy manager and the security officer.
            (1) If needed, the decision may be elevated to the full data governance committee.
        ii) A currently approved alternative exists.
            (1) To protect sensitive information, the district limits the number of software solutions through which this data can be accessed. Access is restricted to the minimum number of platforms required to accomplish essential instructional and administrative tasks.
            (2) Decisions based on the availability of an existing, approved solution may be appealed by submitting a request to the Executive Director of Teaching and Learning.
                (a) The appeal will then be presented to the Instructional Council for a final determination.
                (b) An appeal cannot override a privacy or security denial.

iii) The security officer OR student data privacy officer subjectively determines, based on professional opinions, that the request may cause harm or loss of data to the district, staff, or students.
iv) Teaching and learning determines the request does not align with district standards.

3) **Limits**
    a) Software requests shall be reviewed only once per school year for each requested solution.
        i) Reasonable exceptions may be made when relevant capabilities, terms, or the software's security have changed.
4) **Non-Compliance**
    a) Circumventing the formal software approval process to use an unapproved digital resource that handles protected Class I or Class II data constitutes a serious policy violation.
    b) Such actions shall result in a referral to human resources for potential disciplinary proceedings.
    c) To maintain the security and integrity of district systems, installing any unapproved software on district resources is prohibited, regardless of whether it handles protected data.

District-Wide Software Adoption

Software adoption that affects the entire district or a large portion of it should be thoroughly reviewed by designated technology experts during the RFP or other processes.

1) RFP committees should include one or more technology experts in at least one of the following areas:
    a) RFP requirement development,
    b) initial screening team, or
    c) RFP selection committee.
2) Adoptions that integrate with one of the district's data sources must involve a relevant technology expert, regardless of whether a formalized RFP or state purchasing process is in place.
3) Total cost of ownership for supporting and maintaining district-wide software adoptions should be considered, including training, ongoing help desk support, and other data maintenance tasks.

Updated: October 15, 2026