



Secure Access


If users want to access the practice and training tests as a TA or TE—required for the use of the text-to-speech accessibility resource—a logon will be required. TAs and TEs can contact their CAASPP test site coordinator for logon credentials.


Technology Resources

The *CAASPP and ELPAC Technical Specifications and Configuration Guide for Online Testing* ([/tech-specs-and-config/](#)),  provides technology coordinators information about supported technology and technology requirements and can be used to confirm that the school meets the minimum requirements for computer-based testing with the technical specifications for computer-based testing, including the following:

- Information about internet and network requirements
- Hardware and software requirements
- Secure browser installation
- Supported operating systems for student testing
- Supported web browsers
- Supported peripheral equipment for testing

The *Bandwidth Checker* (https://demo.tds.cambiumast.com/systemdiagnostic/pages/default.aspx?c=California_PT&url=https://capt.tds.cambiumast.com/student),  web page can assist technology coordinators to assess network readiness by performing a real-time check of a school's network bandwidth. Note that technology coordinators may want to run this test more than once and at different times of the day because estimates change as the network conditions change and can vary from run to run.

The CDE also hosts a *Smarter Balanced Technology Readiness Resources* (<https://www.cde.ca.gov/ta/tg/sa/sbac-ittr-index.asp>),  web page, which includes links to tools, requirements, and topics that LEAs will find useful in planning for the computer-based CAASPP testing.

Finally, the *Smarter Balanced Guide to Technology Readiness* (PDF), (<https://portal.smarterbalanced.org/library/en/guide-to-technology-readiness.pdf>),  web document is intended to help school leaders better understand, plan for, and manage the technology necessary for successful administration of Smarter Balanced assessments. It is intended to help school leaders address key questions about technology readiness for the Smarter Balanced assessment system, including what it means to be “technology ready” for the Smarter Balanced assessments.

Security of the Test Environment

A secure online testing environment is possible when an individual is restricted from accessing prohibited computer applications (local or internet-based) or copying or otherwise sharing test data. A secure online testing environment is necessary to maintain test security and provide a stable testing experience for students across multiple platforms. The security of assessment instruments and the confidentiality of student information are vital to maintaining the validity, reliability, and fairness of the results.

All summative test items and test materials are secure and must be appropriately handled. Secure handling protects the integrity, validity, and confidentiality of assessment items, prompts, student information, and test results. Any deviation in test administration must be reported as a test security incident to ensure the validity of the assessment results.

It is the responsibility of each person participating in the administration of any of the CAASPP summative assessments to immediately report any violation or suspected violation of test security or confidentiality. The CAASPP test site coordinator is responsible for immediately reporting any security violation to the LEA CAASPP coordinator.

Note regarding student cheating: In the case of a student cheating, the TA must stop the cheating; however, if the incident of cheating does not involve electronic devices, the LEA may decide to allow the student to complete the remainder of the test. After testing, the TA must notify the CAASPP test site coordinator. **Do not call** the CDE, an LEA Success Agent, or CalTAC to report student cheating. The LEA CAASPP coordinator or CAASPP test site coordinator must, instead, file a report using the STAIRS/Appeals process.

If the LEA decides to allow the student(s) to complete testing, the LEA CAASPP coordinator or CAASPP test site coordinator should open a STAIRS case in TOMS immediately with the incident type of “Student Cheating or Accessing Unauthorized Devices” and the *Yes, I want the student to complete the assessment* radio button selected. The STAIRS case remains in Draft status until the student has completed testing, when the submitter can return to file an Invalidate Appeal.

Requirements



NOTE: Because of the nature of the CAAs for ELA, mathematics, and science, TEs are permitted exposure to test questions and student responses. Additionally, in some cases, TEs will enter student responses into the TDS as indicated by the student’s IEP.

TAs, TEs, and CAASPP test site coordinators or other individuals who have witnessed, been informed of, or suspect the possibility of a test security incident that could potentially affect the validity of inferences from test results or the integrity of the assessments or the data should review the information in the subsections [Identifying Testing Improproprieties, Irregularities, and Breaches \(/caaspp-otam/test-security/identifying-testing-incidents/#improprieties-irregularities-breaches\)](#) and [Appeals Submission \(/caaspp-otam/test-security/identifying-testing-incidents#appeals-](#)




submission), (as necessary) of this manual; and then refer to the *CAASPP and ELPAC Security Incidents and Appeals Procedure Guide (/stairs/)*  for additional instructions. Note that only LEA CAASPP coordinators and CAASPP test site coordinators may report the incident using the STAIRS/Appeals process and, if directed, file an Appeal.

Table 1 through table 4 describe security requirements for the test environment during various stages of testing. The test environment refers to all aspects of the testing situation while students are testing and includes what a student can view, hear, or access (including access via technology).

Before Testing


Table 1. Requirements of the Test Environment Before Testing

Requirement	Description
Instructional materials removed or covered	Instructional materials must be removed or covered, including, but not limited to , information that might assist students in answering questions that is displayed on bulletin boards, chalkboards or dry-erase boards, or on charts (e.g., wall charts that contain literary definitions, maps, mathematics formulas, etc.).
Student seating	Students must be seated to minimize opportunities to look at each other’s work—for example, students may be assigned staggered seating or be seated in every other chair or workstation position—or they should be provided with tabletop partitions.
Signage	Place a <u>“TESTING IN PROGRESS-DO NOT DISTURB”</u> (PDF) (https://www.caaspp.org/rsc/pdfs/calif-tac-do-not-disturb-sign.pdf)  sign on the door or post signs in halls and entrances rerouting hallway traffic, as well as an <u>“Unauthorized Electronic Devices May Not Be Used at Any Time During the Testing Session”</u> (PDF) (https://www.caaspp.org/rsc/pdfs/calif-tac-unauthorized-electronic-devices-sign.pdf)  sign in the testing environment, to promote optimum testing conditions.

During Testing

Table 2. Requirements of the Test Environment During Testing

Requirement	Description
Quiet environment	Provide a quiet environment void of talking or other distractions that might interfere with a student’s ability to concentrate or might compromise the testing situation or environment.

Requirement	Description
Student supervision	<p>Students are actively supervised by a trained TA or TE and are prohibited from</p> <ul style="list-style-type: none"> • viewing other students' answers; • distracting or interrupting other students; and • accessing or using unauthorized electronic devices that allow access to outside information, communication among students or with other individuals outside the testing environment, or the ability to photograph or copy test content. This includes any device with cellular, messaging, or wireless capabilities, but is not limited to cell phones, smart watches, personal digital assistants, tablets, iPods or other mp3 devices, cameras, and electronic translation devices.
Access to allowable resources only	<p>Students must only have access to and use of those allowable resources (refer to the subsection <i>Establishing Appropriate Testing Conditions</i> (/caaspp-otam/ta-interface/about-testing/#establishing-appropriate-test-conditions) for examples) that are permitted for each specific test (or portion of a test). This includes access to medical supports and devices that may be integrated into other technology devices (refer to the <i>Smarter Balanced Usability, Accessibility, and Accommodations Guidelines</i> (PDF), (https://portal.smarterbalanced.org/library/en/usability-accessibility-and-accommodations-guidelines.pdf),  for information about student use of medical supports during testing). Use of such devices may require additional monitoring or a separate test setting to maintain test security.</p>
Access to assessments	<p>Unauthorized staff or other adults (including students' parents/guardians) must not be in the room during testing. Only students who are testing can view items. Based on the item type (i.e., PTs), trained TAs may also have limited exposure to items in the course of properly administering the assessments; however, even TAs or TEs and other trained staff must not actively review, record, or analyze any test items. However, TEs administering the CAAs will have exposure to test items in the course of properly administering the assessments.</p>
Testing through secure browser	<p>Administration of the CAASPP assessments is permitted only through the student interface via a secure browser or a method of securing the student device.</p>

During and After Testing

Table 3. Requirements of the Test Environment During and After Testing

Requirement	Description
-------------	-------------

Requirement	Description
No access to responses	LEA CAASPP coordinators, CAASPP test site coordinators, TAs, and other staff are not permitted to review student responses to the Smarter Balanced assessments, CAST, or CSA in the testing interface or students' notes on scratch paper.
No copies of test materials	Unless needed as a print-on-demand or braille accommodation, no copies of the test items, stimuli, reading passages, PT materials, or writing prompts may be made or otherwise retained.
No access to digital, electronic, or manual devices	No digital, electronic, or manual device may be used to record or retain test items, reading passages, or writing prompts. Similarly, these materials must not be discussed with or released to anyone via any media, including fax, email, text message, social media websites, etc.
No retaining, discussing, or releasing test materials	Descriptions of test items, stimuli, printed reading passages, or writing prompts must not be retained, discussed, or released to anyone.
No reviewing, discussing, or analyzing test materials	LEA CAASPP coordinators, CAASPP test site coordinators, TAs, and other staff must not review, discuss, or analyze test items, stimuli, reading passages, or writing prompts at any time, including before, during, or after testing. Student interaction with a TA or TE during a test is limited to necessary communication (such as permission to leave the room) or to respond during any CAA. Students should be informed that they may not discuss or share test items, stimuli, reading passages, or writing prompts with anyone during or after testing.
Keeping all test materials secure at all times	Printed materials from the print-on-demand accommodation, scratch paper, the CAA <i>DFA(s)</i> , and documents with student information must be securely stored in a locked location (e.g., locked room closet or cabinet) that can be opened only with a key or keycard by staff responsible for test administration.
No retaining of test “tickets” or any materials created to assist students with logging on to the summative assessments	All students' ID information must be collected at the end of each test session, stored securely, and then destroyed securely.

After Testing


Table 4. Requirements of the Test Environment After Testing


Requirement	Description
-------------	-------------

Requirement	Description
No test materials used for instruction	Test items, stimuli, reading passages, or writing prompts must not be used for instruction.
Destroy test materials securely	Printed test items or passages, including embossed braille printouts, scratch paper, notecards or paper that include student logon information, and printed <i>DFA(s)</i> for the CAAs must be collected and inventoried and then immediately shredded upon a student's completion of the test. Refer to the next subsection, <i>Handling Secure Printed Materials (/caaspp-otam/test-security/secure-printed-materials/)</i> , for details.

Handling Secure Printed Materials

Using Print-on-Demand Materials

For those students whose IEP or Section 504 plan expresses a need for a paper copy of **passages or items**, permission for the students to receive this accommodation must be requested by the LEA CAASPP coordinator at least two weeks prior to testing by contacting the [LEA Success Agent \(/contact/lea-success-agents/\)](/contact/lea-success-agents/). .

Printing **individual test items** for students with this accommodation will require that the LEA CAASPP coordinator make a request to the [LEA Success Agent \(/contact/lea-success-agents/\)](/contact/lea-success-agents/).  to have the accommodation set for each student in addition to assigning this resource for the student in TOMS.

Note the following about print-on-demand:

- Print requests must be approved and processed by the TAs and TEs during test administration.
- The decision to allow students to use print-on-demand must be made on an individual student basis and is available only for students with an IEP or Section 504 plan.
- Because items are printed individually, using the print-on-demand functionality does not allow a printed version of the computer-based test to be created prior to testing, especially given the adaptive nature of the Smarter Balanced assessments.
- A very small percentage of students should need this accommodation.
- The use of this accommodation may result in the student needing additional time to complete the assessment.

Once a student is approved to receive the printing of test items or passages for Smarter Balanced assessments, the CAST, or the CSA, that student may send a print request to the TA during testing by selecting the [**Print**] icon on the screen. For the CAAs, the TE may select this icon. This request needs to be made for each individual item.

Follow these guidelines when using the print-on-demand accommodation:

1. Before the TA or TE approves the student's request to print a test item or stimulus, the TA or TE must ensure that the printer is on and is monitored by staff who have been trained.
2. Immediately after printing a print-on-demand request, the file should be securely deleted from the TA's or TE's device in such a way that the file does not remain in a temporary storage file where it can be undeleted. Refer to the [Destroying Electronic Files \(/caaspp-otam/test-security/secure-printed-materials/#destroying-electronic-files\)](/caaspp-otam/test-security/secure-printed-materials/#destroying-electronic-files) subsection for additional instructions.
3. The TA or TE must collect the previously printed item from the student after the next item's print request. Printed items must be securely stored and then securely destroyed after the test session.

Using and Securely Destroying Scratch Paper for PTs

Use:

- The only exception to the requirement governing the immediate destruction of printed materials and scratch paper is when students take notes or draft responses to ELA, mathematics, or science PTs.
- During the Smarter Balanced ELA PT, the notes on the embedded universal tool, global notes, are retained from Part 1 to Part 2 so that the student may return to the notes even though the student is not able to go back to specific items in Part 1. The embedded global notes is the preferred mode for notetaking during the Smarter Balanced ELA PT.
- Students may also use scratch paper to make notes or develop draft responses. To maintain the security of scratch paper used for notes on the ELA or mathematics PTs, or CAST, CAA, or CSA questions, TAs or TEs must direct students to write their names (or some appropriate identifying information) on their scratch paper, and then collect and inventory the scratch paper at the end of each test session, as well as upon completion of the test to maintain test security. The retention of scratch paper (including graph paper) is allowed for the PTs, CAST, CAAs, and CSA.
- **Do not** keep printed test items or passages or scratch paper for future test sessions except as noted for PTs.

Destroying Secure Printed Materials

Printed materials from the print-on-demand accommodation, CAA *DFAs*, answer-recording documents, and scratch paper must be kept in a securely locked room or locked cabinet that can be opened only with a key or keycard by staff who are responsible for test administration and who have signed a *CAASPP Test Security Affidavit*. All test materials must remain secure at all times.

Printed test items or passages, including embossed braille printouts and scratch paper, must be collected and inventoried at the end of each test session and then immediately destroyed securely according to LEA and CAASPP policies or procedures.

CAA DFAs that were printed for TEs after being downloaded from the password-protected TOMS website must be kept in a securely locked room or locked cabinet when not in use. Once testing is completed, these must be immediately securely destroyed according to LEA policies and procedures, California policies and procedures, or policies and procedures from both sources.

Answer-recording documents used to complete second scoring for the CAA for ELA must be kept securely.

Destroying Electronic Files

Immediately after printing a print-on-demand request or making a printed copy of a *DFA* for the CAAs, the file produced by the process should be securely deleted from the location on which it was stored. If stored on a device, the device on which the files are stored must be kept in a securely locked room or locked cabinet while the secure files exist.


A file(s) must be deleted in such a way that the file does not remain in a temporary storage location such as Windows' Recycle Bin, where it can be undeleted. TAs, TEs, and CAASPP test site coordinators should use the school's or LEA's preferred method of secure file deletion.

While there are many ways to permanently delete a file, including using a “shredding” tool that might be part of a virus scanning tool, what follows are basic ways to remove a file from a Windows or Macintosh system:

- **Windows**—Hold the [Shift] key when deleting the file or empty the Recycle Bin after deleting.
- **Macintosh and Macintosh equivalent devices using OS X or macOS**—Press the [Command] + [Delete] keys with any file or folder selected to send a file to the Trash and then press the [Shift] + [Command] + [Delete] keys *or* open the Finder menu and then select “Secure Empty Trash” to immediately empty the Trash.

Identifying Testing Improprieties, Irregularities, and Breaches



NOTE: The processes described in this section are to be used to report incidents for the CAASPP computer-based assessments only. Refer to the *CAASPP Paper–Pencil Testing Test Administration Manual* (</caaspp-ppt-tam/>).  for the special version (braille or large-print) assessment being administered for what to do in the event of an incident that occurs during this testing.

Test security incidents, such as improprieties, irregularities, and breaches, are behaviors prohibited either because they give a student an unfair advantage, compromising the validity of inferences from student test results, or because they compromise the secure administration of the assessments. Whether intentional or accidental, failure to comply

with security and administration rules, either by staff or students, constitutes a test security incident. Improprieties, irregularities, and breaches must be reported in accordance with the instructions in this section for each severity level.

Some incidents may require that an Appeal be submitted to reset, reopen, restore (if a test had been reset in error), provide a grace period extension, or invalidate a test. LEA CAASPP coordinators or CAASPP test site coordinators can make the determination by reporting the incident using the online CAASPP STAIRS/Appeals process in TOMS.

The STAIRS/Appeals Process

NOTES:



- The STAIRS/Appeals process must be used to report incidents that occur during the administration of the Smarter Balanced Summative Assessments, the CAAs, the CAST, and the CSA.
- Incidents that occur during the administration of the interim assessments are handled at the local level and should not be reported using the STAIRS/Appeals process.
- Testing incidents can only be reported in STAIRS within the LEA's selected testing window and should be filed with enough time for students to finish testing after an Appeal has been granted.

The online STAIRS/Appeals process, which is available in TOMS and described in the [*CAASPP and ELPAC Security Incidents and Appeals Procedure Guide \(/stairs/\)*](#), must be used by LEA CAASPP and CAASPP test site coordinators to report a confirmed test security incident or other testing issue that interferes with the administration and completion of the assessment.


LEA CAASPP coordinators and CAASPP test site coordinators must ensure that all test security incidents are documented using the STAIRS/Appeals process in TOMS **within 24 hours of the incident**.

After the incident is reported, TOMS will immediately prompt the filing of an Appeal if that is the appropriate action. A system email will be sent that describes the submittal and includes the case number that can be used for searches in TOMS. This email will be sent to the submitter (and to the LEA CAASPP coordinator, if the STAIRS case or the Appeal is submitted by the CAASPP test site coordinator).

LEA CAASPP coordinators must view the announcements and to-do list in the “MyTOMS at a Glance” section of their home page in TOMS. TOMS sends an automated notification to the LEA if there are any STAIRS cases that have a Draft status and need to be submitted shortly before the LEA's testing window closes.

STAIRS cases with any status—draft, partial CDE approval, partial CalTAC approval, pending CDE approval, pending CalTAC approval, and completed—are searchable in *Search STAIRS* in TOMS. Appeals with any status—approved, pending, pending approval, rejected (*Appeals rejected by the CDE or CalTAC*), rejected by system, swap approved, and withdrawn—are searchable in *Search Appeals* in TOMS.


Incident Definitions and Action Steps

Refer to the [CAASPP and ELPAC Security Incidents and Appeals Procedure Guide \(/stairs/\)](/stairs/)  for details about the incident reporting process and a detailed description of the STAIRS process.


After an incident has occurred, the **CAASPP test site coordinator** is responsible for reviewing and verifying the details of the incident and immediately notifying the LEA CAASPP coordinator of any security breaches or testing irregularities that occur before, during, or after summative testing. Depending on the LEA's procedure, it is either the LEA CAASPP coordinator or the CAASPP test site coordinator who submits the incident using the STAIRS/Appeals process, and then it is the LEA CAASPP coordinator who opens the STAIRS case.

If the incident is a breach, the LEA CAASPP coordinator should be informed immediately; it is the LEA CAASPP coordinator who will initiate action. If the incident is due to social media exposure on the part of a student or adult or to media coverage of an administration, the LEA CAASPP immediately contacts CalTAC by phone at 800-955-2954 to report it.

The LEA CAASPP coordinator will also respond to and assist the CDE and test security personnel, as requested. Any documentation associated with the incident should be kept for at least one year.

The online data-entry screens used during the STAIRS/Appeals process in TOMS prompt the user through the steps necessary to submit a STAIRS case. The [CAASPP and ELPAC Security Incidents and Appeals Procedure Guide \(/stairs/\)](/stairs/)  lists the incident types and any action to be taken.



NOTE: LEA CAASPP coordinators should contact CalTAC if the incident does not meet any of the criteria described in the [CAASPP and ELPAC Security Incidents and Appeals Procedure Guide \(/stairs/\)](/stairs/) .



WARNING: The user **must** select the [SUBMIT] button as the last step of the STAIRS/Appeals data-entry screen in TOMS, which is the final step in the STAIRS/Appeals process. Otherwise, the entry will be saved as a draft.

Impropriety

An impropriety is an unusual circumstance that has a low impact on the individual or group of students who are testing and has a low risk of potentially affecting student performance on the test or of impacting test security or test validity. These circumstances can be corrected and contained at the local level. An example of an impropriety could be if student(s) were making distracting gestures or sounds or talking during the test session that creates a disruption in the test session for other students, or a student or students left the test room without authorization.

The steps to process an impropriety are as follows:

1. Local administrators or staff take corrective action, where necessary, and notify the site coordinator.
2. The incident is mitigated as necessary by school staff, and the LEA CAASPP coordinator is contacted for assistance with mitigation as necessary.
3. The CAASPP test site coordinator or LEA CAASPP coordinator reports the impropriety using the online STAIRS/Appeals process in TOMS **within 24 hours**.

Irregularity

An irregularity is an unusual circumstance that impacts an individual or group of students who are testing and may potentially affect student performance on the test or impact test security or test validity. These circumstances can be contained at the local level. An example of an irregularity could be that student(s) were assigned an incorrect designated support or accommodation, or student(s) cheated or provided answers to each other.

The steps to process an irregularity are as follows:

1. Local administrators or staff take corrective action and notify the site coordinator.
2. The incident is mitigated as necessary by school staff, and the LEA CAASPP coordinator is notified for assistance with mitigation.
3. The CAASPP test site coordinator or LEA CAASPP coordinator reports the irregularity using the online STAIRS/Appeals process in TOMS **within 24 hours**.
4. The coordinator submits an Appeal request through STAIRS, if prompted.
5. The submitter (and the LEA CAASPP coordinator, if the submitter was a CAASPP test site coordinator) receives an email summarizing the STAIRS case.
6. The CDE or the ETS LEA Administrator reviews the STAIRS case and approves the Appeal, if necessary. The coordinator retains the STAIRS response email for the record.

Breach

A breach is a test administration event that poses a threat to the validity of the test. These circumstances have external implications for the CDE, the Smarter Balanced Assessment Consortium, or both, and may result in a decision to remove the test item(s) from the available secure bank.

Breaches require **immediate** attention and escalation **by the LEA CAASPP coordinator calling CalTAC at 800-955-2954** if the breach is due to social media exposure on the part of a student or adult, or media coverage of a test administration. Following the call, the CAASPP test site coordinator or LEA CAASPP coordinator must report the breach using the STAIRS/Appeals process within 24 hours.

Examples may include such situations as exposure of secure materials, a repeatable security or system risk, a TA modifying student answers, or test items were shared on social media. These circumstances have external implications.

The steps to process a breach are as follows:

1. Local administrators or staff mitigate the incident as necessary and immediately report the breach to the CAASPP test site coordinator, LEA CAASPP coordinator, or both.
2. LEA staff members investigate the security risk and alert the LEA Success Agent or CalTAC for social media breaches and stand ready to receive further guidance on the dispensation of the event.
3. The LEA CAASPP coordinator immediately calls the LEA Success Agent or CalTAC to report the breach. Following the call, the CAASPP test site coordinator or LEA CAASPP coordinator reports the breach using the online STAIRS/Appeals process in TOMS within 24 hours.
4. The coordinator submits an Appeal request through STAIRS, if prompted.
5. The submitter (and the LEA CAASPP coordinator, if the submitter was a CAASPP test site coordinator) receives an email summarizing the submittal.
6. The CDE reviews the STAIRS case and approves the Appeal, if necessary. The coordinator retains the STAIRS response email for the record.

Appeals Submission

An incident must first be reported by the LEA CAASPP coordinator or CAASPP test site coordinator using the STAIRS/Appeals process in TOMS. If an Appeal is to be filed, the data-entry screen will provide the appropriate prompts.

NOTES:

- LEA CAASPP coordinators must contact CalTAC to make a request in STAIRS to restore a test that has been reset by the LEA in error. Only CalTAC can submit a STAIRS case for a