Chapter 3. Test Security

Additional Resource for This Chapter:

- CAASPP List of Acronyms and Initialisms web page—
  http://www.caaspp.org/about/abbreviations.html

2019–2020 TEST ADMINISTRATION

CAASPP Online Test Administration Manual

caaspp
California Assessment of
Student Performance and Progress

- Smarter Balanced for English Language Arts/Literacy and Mathematics Summative Assessments
- California Alternate Assessments for English Language Arts/Literacy, Mathematics, and Science
- California Science Test
- California Spanish Assessment

© California Department of Education
Prepared by Educational Testing Service ®
Posted January 2020

ETS
Measuring the Power of Learning.

Security of the Test Environment

> **Resources in This Section:**
> - CAASPP Security and Test Administration and Incident Reporting System Process (STAIRS)/Appeals Process for Summative Assessments web page— http://www.caaspp.org/stairs/
> - CAASPP Manuals and Instructions web page—http://www.caaspp.org/administration/instructions/
> - *CAASPP Security Incidents and Appeals Procedure Guide* web document— http://www.caaspp.org/rsc/pdfs/CAASPP.stairs-appeals-guide.2019-20.pdf

A secure online testing environment is a state in which a device is restricted from accessing prohibited computer applications (local or internet-based), or copying or otherwise sharing test data. The purposes of this environment are 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, and student information. 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.

In the case of a student cheating, the test administrator must stop the cheating; however, the student may be allowed to complete the remainder of the test. After testing, the test administrator must notify the CAASPP test site coordinator. **Do not call** the CDE 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 and keep the STAIRS case in Draft status. The LEA shall receive an email from ca-assessments@ets.org instructing to submit the delayed appeal once student completes testing.

Requirements

> **Note:** Due to the nature of the CAAs for ELA, mathematics, and science, test examiners are permitted exposure to test questions and student responses. Additionally, in some cases, test examiners will enter student responses into the test delivery system as indicated by the student's IEP.

Test administrators, test examiners, 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 integrity of the assessments or the data should review the information in the subsections *Identifying Testing Improprieties, Irregularities, and Breaches* and *Appeals* (as necessary) of this manual; and then refer to the *CAASPP Security Incidents and Appeals Procedure Guide* web document 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, an Appeal.

Table 2 through Table 5 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 see, hear, or access (including access via technology).

Before Testing

Table 2. 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 so there is enough space between them 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 table-top partitions.

Table 2 *(continuation)*

Requirement	Description
Signage	If helpful, place a "TESTING—DO NOT DISTURB" sign on the door or post signs in halls and entrances rerouting hallway traffic in order to promote optimum testing conditions.
	CAASPP test site coordinators or test administrators should post the "Unauthorized Electronic Devices May Not Be Used at Any Time During the Testing Session" signs so that they are clearly visible to all students. A master of this sign can be downloaded from the Manuals and Instructions web page on the CAASPP website.

During Testing

Table 3. 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.
Student supervision	Students are actively supervised by a trained test administrator or test examiner and are prohibited from access to unauthorized electronic devices that allow availability to outside information, communication among students or with other individuals outside the testing environment, or photographing or copying 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, cameras, and electronic translation devices.

Table 3 *(continuation)*

Requirement	Description
Access to allowable resources only	Students must only have access to and use of those allowable resources (refer to the subsection *Establishing Appropriate Testing Conditions* for examples) that are permitted for each specific test (or portion of a test). This includes access to medical supports, which may be integrated into other technology devices. Use of such devices may require additional monitoring or a separate test setting to maintain test security.
Access to assessments	Unauthorized staff or other adults 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 test administrators may also have limited exposure to items in the course of properly administering the assessments; however, even test administrators or test examiners and other trained staff must not actively review or analyze any test items.
Testing through secure browser	Administration of the CAASPP assessments is permitted only through the student interface via a secure browser or a method of securing the student device.

During and After Testing

Table 4. Requirements of the Test Environment During and After Testing

Requirement	Description
No access to responses	LEA CAASPP coordinators, CAASPP test site coordinators, test administrators, 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.

Table 4 *(continuation)*

Requirement	Description
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, test administrators, 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 test administrator or test examiner 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 *DFA(s),* and documents with student information must be kept in a securely locked room or locked 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 5. Requirements of the Test Environment After Testing

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 *DFA(s)* 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, *Handling Secure Printed Materials*, for details.

Handling Secure Printed Materials

Secure Handling of 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 CalTAC.

Printing **individual test items** for students with this accommodation will require that the LEA CAASPP coordinator make a request to CalTAC 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 test administrators and test examiners 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, utilizing the print-on-demand functionality does not allow a printed version of the online 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, CAST, or CSA, that student may send a print request to the test administrator during testing by selecting the print icon on the screen. For the CAAs, the test examiner 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 test administrator or test examiner approves the student's request to print a test item or stimulus, the test administrator or test examiner 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 test administrator's or test examiner'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* subsection for additional instructions.

3. The test administrator or test examiner 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.

Destroying Secure Printed Materials

Printed materials from the print-on-demand accommodation, CAA *DFA*, 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 responsible for test administration 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 securely destroyed according to LEA and California policies or procedures.

CAA *DFAs* that were printed for test examiners after being downloaded from the password-protected TOMS 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.

Destroying Electronic Files

Immediately after printing a print-on-demand request, making a printed copy of a *DFA* for the CAAs, the file produced by the process should be securely deleted from the test administrator's or test examiner's device. It 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. Test administrators, test examiners, 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**—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.

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 note taking 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, test administrators or test examiners 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. The retention of scratch paper (including graph paper) is allowed for the PTs, the CAST, CAAs, and CSA.

- **DO NOT** keep printed test items or passages or scratch paper for future test sessions except as noted for PTs.

> ⚠️ **Caution: The retention of scratch paper is only allowed for the Smarter Balanced PTs, CAST, CAAs, and CSA.** At the end of each test session, all scratch paper (including graph paper) must be collected, inventoried, and securely stored for student use in a subsequent test session. All scratch paper must be securely destroyed immediately upon the student's completion of the test to maintain test security.

Identifying Testing Improprieties, Irregularities, and Breaches

> **Note:** The processes described in this section are to be used to report incidents for the CAASPP online assessments only. Refer to the *CAASPP Paper-Pencil Testing Test Administration Manual* 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 or because they compromise the secure administration of the assessments. Whether intentional or by accident, failure to comply with security and administration rules, either by staff or students, constitutes a test security incident. Improprieties, irregularities, and breaches need to 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.

After a user has entered the details of the incident, TOMS will prompt the filing of an Appeal during the STAIRS/Appeal process, if that is the appropriate action. A system email will be sent that confirms that the incident was filed.

Impact and Definitions

> **Resources in This Subsection:**
>
> - *CAASPP Security Incidents and Appeals Procedure Guide* web document—
>   http://www.caaspp.org/rsc/pdfs/CAASPP.stairs-appeals-guide.2019-20.pdf

Definitions for test security incidents that can occur during administration of the summative assessments are provided in Table 6. Incidents should be logged using the STAIRS/Appeals process described in the *CAASPP Security Incidents and Appeals Procedure Guide*.

Table 6. Definitions for Test Security Incidents

Incident	Definition
Impropriety	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 impropriety should be reported to the LEA CAASPP coordinator and CAASPP test site coordinator immediately. The coordinator will report the incident **within 24 hours** using the STAIRS/Appeals process.
Irregularity	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 corrected and contained at the local level. An irregularity must be reported to the LEA CAASPP coordinator and CAASPP test site coordinator immediately. The coordinator will report the irregularity **within 24 hours**, using the STAIRS/Appeals process to both report the incident and file the Appeal.

Table 6 *(continuation)*

Incident	Definition
Breach	An event that poses a threat to the validity of the test. Examples may include such situations as a release of secure materials or a security or system risk. These circumstances have external implications for the CDE, the Smarter Balanced Assessment Consortium, or both, and may result in a Consortium decision to remove the test item(s) from the available secure bank. A breach incident must be reported to the LEA CAASPP coordinator immediately.
	The LEA CAASPP coordinator must **immediately** report the breach by calling either CalTAC at 800-955-2954 if the breach is due to social media exposure on the part of a student or adult; or the CDE at 916-445-8765 for all other breaches. In addition, the coordinator must report the incident **within 24 hours,** using the STAIRS/Appeals process**.**

It is important for test administrators and test examiners to ensure that the physical conditions in the testing room meet the criteria for a secure test environment. Refer to the subsection *Requirements* for more detail.

Using STAIRS

> **Resources in This Section:**
>
> - CAASPP Security and Test Administration Incident Reporting System (STAIRS) Applicable Testing Incidents Chart web document— http://www.caaspp.org/rsc/pdfs/CAASPP.STAIRS-issues.2019-20.pdf
> - CAASPP website—http://www.caaspp.org/
> - *CAASPP Security Incidents and Appeals Procedure Guide* web document— http://www.caaspp.org/rsc/pdfs/CAASPP.stairs-appeals-guide.2019-20.pdf

The online STAIRS/Appeals process, available in TOMS, must be used by LEA CAASPP and CAASPP test site coordinators to report a test security incident or other testing issue that interferes with the administration and completion of the assessment. Testing incidents must be reported 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.

Breach incidents must be reported by phone to the CalTAC or the CDE whether the LEA's selected testing window is still open or has closed. (Refer to the *CAASPP Security Incidents and Appeals Procedure Guide* web document for details about the incident reporting process.)

LEA CAASPP coordinators and CAASPP test site coordinators must ensure that all test security incidents are documented using the STAIRS/Appeals process in TOMS. 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 form is submitted by the CAASPP test site coordinator). Ensure that communications generated by the email address ca-assessments@ets.org are not automatically sent to a junk mail or spam folder.

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 shall send an automated notification to the LEA if there are any STAIRS cases that have a Draft status and need to be submitted.

The CDE may review a STAIRS case to determine whether the testing issue requires additional action by the LEA.

Required Action Steps

The Test Security Required Action Steps depict the required actions for each test security incident in a process flow diagram format.

Impropriety

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. (Example: Student(s) making distracting gestures or sounds, or talking during the test session that creates a disruption in the test session for other students.*)*

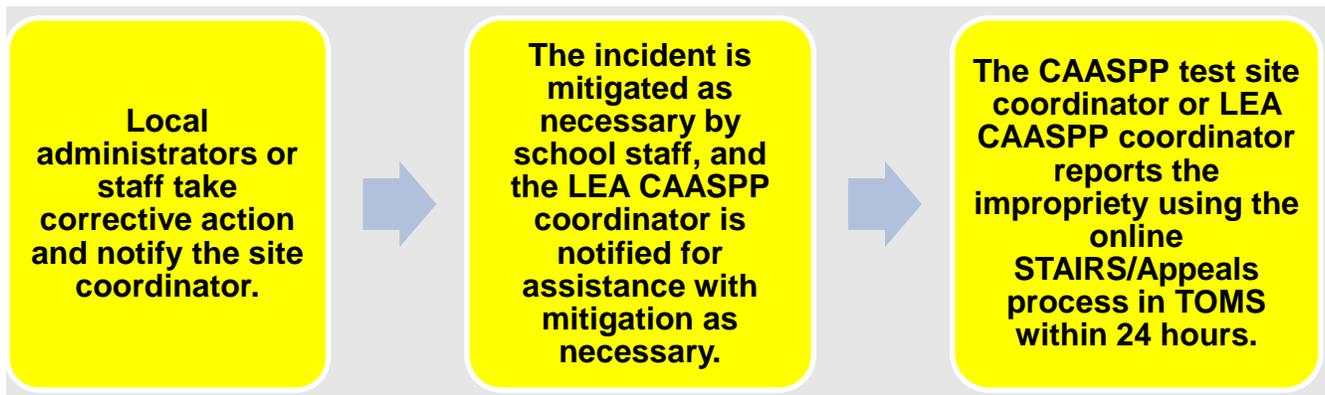The process flow diagram for improprieties is presented in Figure 1.

Figure 1. Impropriety process flow diagram

Irregularity

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. (Example: The test administrator, test examiner, or CAASPP test site coordinator leaves related instructional materials on the walls in a testing room.)

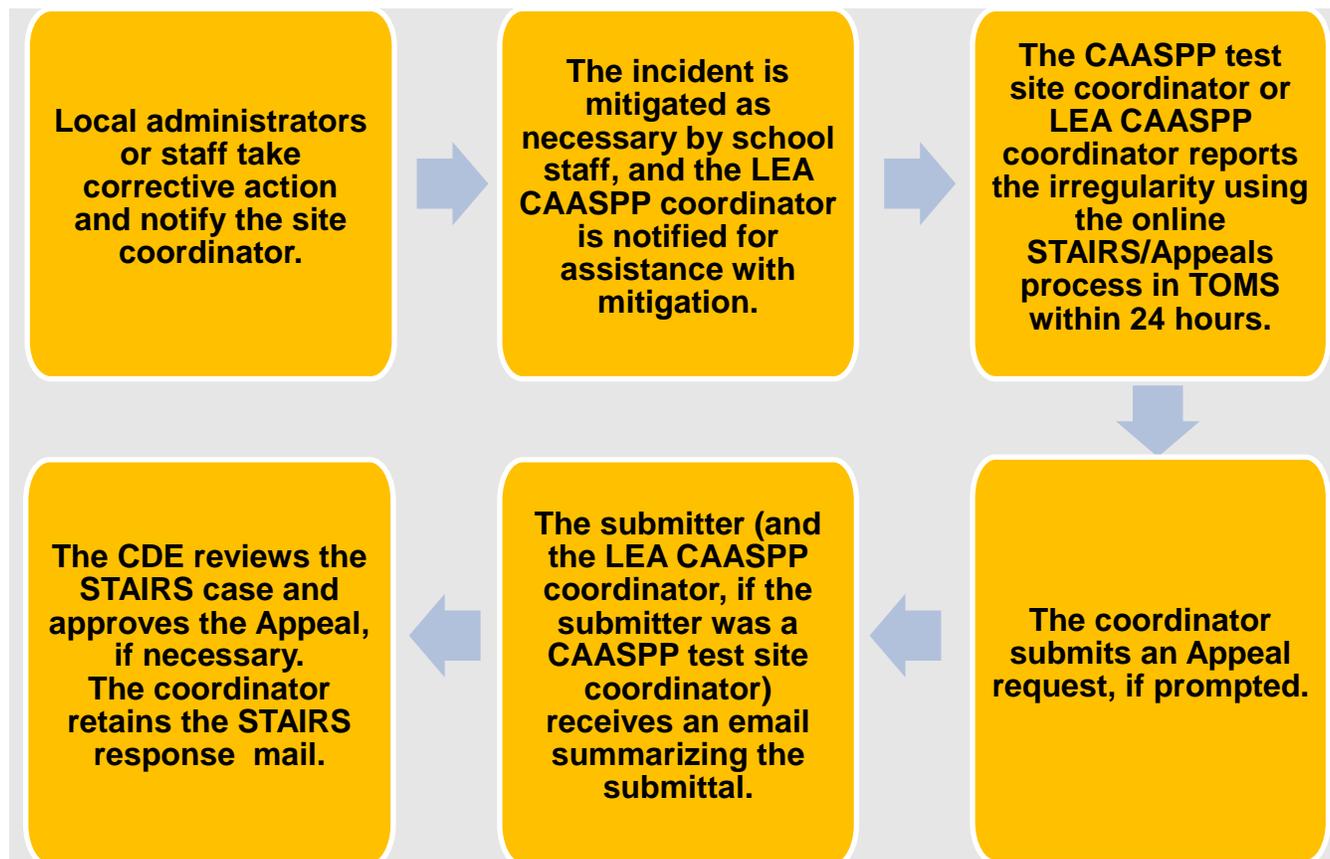The process flow diagram for irregularities is presented in Figure 2.

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

The CDE reviews the STAIRS case and approves the Appeal, if necessary. The coordinator retains the STAIRS response mail. ← The submitter (and the LEA CAASPP coordinator, if the submitter was a CAASPP test site coordinator) receives an email summarizing the submittal. ← The coordinator submits an Appeal request, if prompted.

Figure 2. Irregularity process flow diagram

Breach

*A test administration event that poses a threat to the validity of the test. Breaches require **immediate** attention and escalation **via telephone**—if the breach is due to social media exposure on the part of a student or adult, the LEA CAASPP coordinator contacts CalTAC; for all other breaches, the LEA CAASPP coordinator must contact the CDE. 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 or a repeatable security or system risk. These circumstances have external implications. (Example: Test administrators or test examiners are modifying student answers, or test items are shared on social media.)

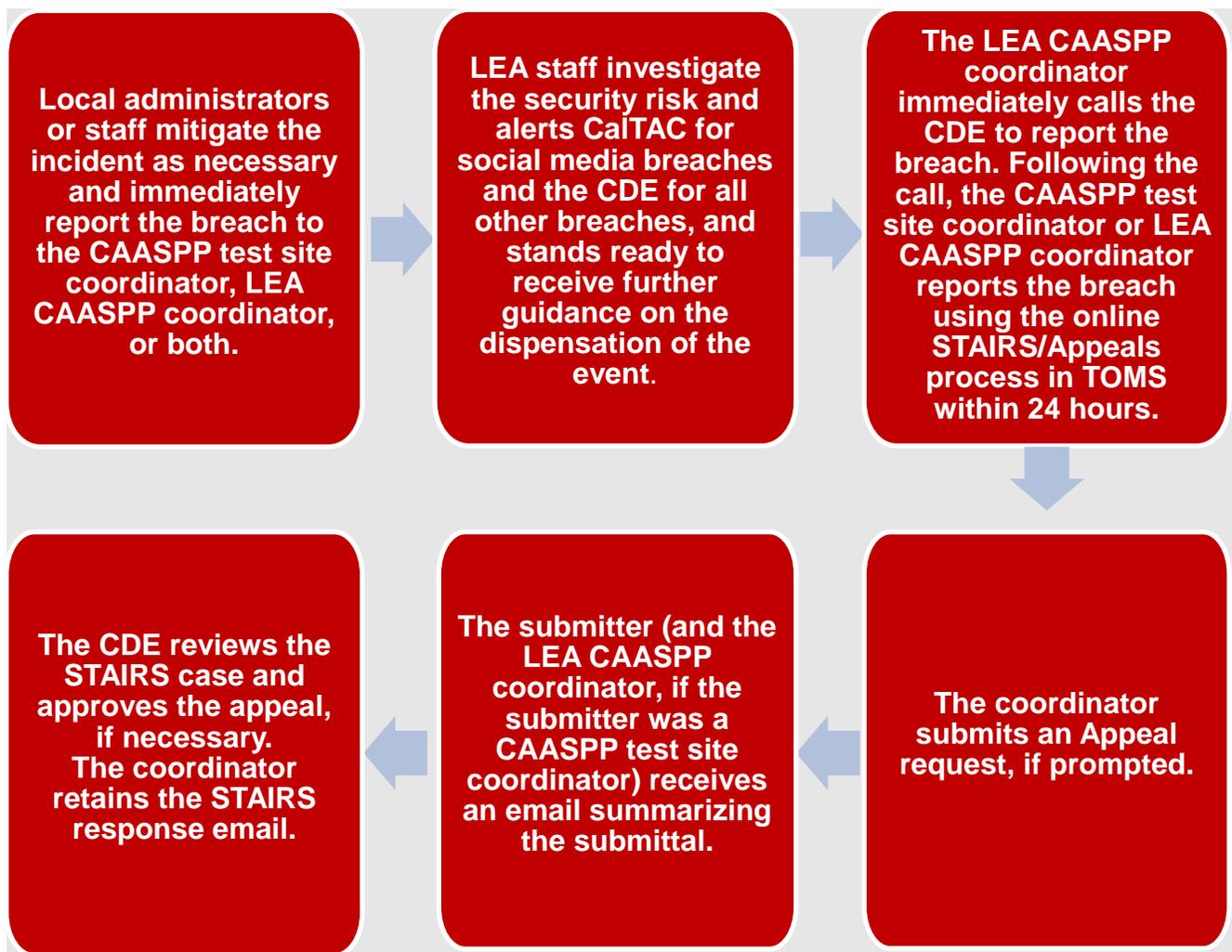The process flow diagram for breaches is presented in Figure 3.

Figure 3. Breach process flow diagram

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.

Information about using the STAIRS/Appeals process is described in the *CAASPP Security Incidents and Appeals Procedure Guide*.

Report Incidents

The LEA CAASPP coordinator is responsible for notifying the CDE **within 24 hours**, using the STAIRS/Appeals process in TOMS, of any incidents that occur before, during, or after summative testing. The CAASPP test site coordinator is responsible for immediately notifying the LEA CAASPP coordinator of any security breaches or testing irregularities that occur in the administration of the test.

The online STAIRS/Appeals process, which is available in TOMS, must be used to provide the required information to the CDE when an incident is confirmed. For cases involving 11 or more students, the STAIRS/Appeals process includes the opportunity to securely upload a spreadsheet containing SSIDs of up to 500 students involved in the irregularity. **Do not upload student names, only SSID numbers.** TOMS will prompt the user if an Appeal is to be filed after the STAIRS case is submitted. When the Appeal type is Invalidate, Grace Period Extension, or a Restore from Reset, the CDE will first review the STAIRS case and approve the Appeal before it is filed in TOMS.

The LEA CAASPP coordinator or CAASPP test site coordinator (with a copy sent to the LEA CAASPP coordinator) submitting the STAIRS case will receive an email to confirm the submittal.

A copy of the email may be sent to the CDE depending on the incident type.

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 CDE or CalTAC)*, rejected by system, swap approved, and withdrawn—are searchable in *Search Appeals* in TOMS.

Coordinator Procedures

The CAASPP test site coordinator:

1. Receives notification of an irregularity

2. Reviews the information provided and verifies that an irregularity has occurred

3. Contacts the LEA CAASPP coordinator and provides all pertinent information *or* reports the incident using the STAIRS/Appeals process, if this is the procedure established for the LEA

The LEA CAASPP coordinator:

1. Receives notification of an irregularity from the CAASPP test site coordinator

2. Reviews the information provided and verifies that the occurrence is an irregularity

3. Acts immediately if the incident type is a breach (Breaches require **immediate** attention and escalation **via telephone—**if the breach is due to social media exposure on the part of a student or adult, the LEA CAASPP coordinator contacts CalTAC; for all other breaches, the LEA CAASPP coordinator must contact the CDE.)

4. Reports the incident using the STAIRS/Appeals process, if this is the procedure established for the LEA

5. Responds to and assists the CDE and test security personnel as requested

6. Keeps any documentation associated with the irregularity for one year

STAIRS Actions

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 Security Incidents and Appeals Procedure Guide* 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 in the STAIRS Applicable Testing Incidents web document.
>
> **Warning:** The user **must** select the [**SUBMIT**] button as the last step of the STAIRS/Appeals data-entry screen in TOMS as the final step in the STAIRS/Appeals process. If it is not, the entry will be saved as a draft.

Appeals

> **Notes***:*
>
> - Do **not** file an Appeal for an interim assessment; the STAIRS/Appeals process is for use with the summative assessments only.
>
> - 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.
>
> - LEA CAASPP coordinators must contact CalTAC to make a request in STAIRS to restore a test that has been reset in error. Only CalTAC can submit a STAIRS case for a Restore Appeal on behalf of the LEA. A Restore Appeal is approved by the CDE.
>
> - A Re-open Appeal cannot be submitted if the test taken by the student has an existing Invalidate Appeal submitted.

Process

An Appeal must be filed before the end of the selected testing window and with enough time to retest the student within the selected testing window. Take the following steps to file an Appeal in TOMS:

1. Document and submit an irregularity or test security incident for a summative assessment using the online STAIRS/Appeals process in TOMS.

2. Review the instructions on the *STAIRS/Appeals > Step 4: Confirm Details* progress step screen before selecting the [**SUBMIT**] button to submit the incident report.

3. If an Appeal is required, the *STAIRS/Appeals > Submit the STAIRS Case to the CDE/File and Appeal* screen appears.

4. Make sure the box in the *Select* column of the "Student Case(s)" table is checked. Enter comments, if any, in the text box, and then select the [**SUBMIT**] button to file the appeal.

5. In cases where the Appeal types are Reset, Reopen, Invalidate, Restore, and Grace Period Extension, and the cases are pending the CDE or CalTAC's approval, the user has the option to cancel the Appeal request by selecting the [**WITHDRAW**] button on the *Summary* screen.

6. The user can make a partial or selective withdrawal by selecting only those SSID(s) in the *Select* column to be removed from the STAIRS case. Once an Appeal has been approved, it cannot be withdrawn.

7. A withdrawn Appeal cannot be processed. If the user wants to report the testing incident for the withdrawn SSID(s), a new STAIRS case must be submitted.

8. A STAIRS case can also be submitted for a nonappealable testing event such as "Incorrect SSID Used," in which the test was completed and the LEA wants to associate the assessment results with the SSID of the student. In this case, the STAIRS case is auto approved. However, the CAASPP test site coordinator must contact the LEA CAASPP coordinator within **one business day** and provide the incorrect SSID, correct SSID, result ID, and test status. The LEA CAASPP coordinator must contact CalTAC within **one business day** by phone at 800-955-2954 or email at caltac@ets.org with the incorrect SSID, correct SSID, result ID, and test status information associated with this incident.

9. In all cases, TOMS will send an email summarizing the STAIRS filing that includes a case number to be used for searches and communications.

An Appeal is processed within four business days of its receipt. Users will receive an email verifying that the Appeal has been processed.

Appeals with any status are searchable in TOMS.

This page is left blank intentionally.