Measuring the Power of Learning.™

California Assessment of Student Performance and Progress (CAASPP)

2015–16 Test Security Guidelines

March 9, 2016
1 – 2:30 p.m.

Agenda

- Introductions
- Requirements in the Testing Regulations
- General Test Security Guidelines
- Specific Test Security Guidelines
- Social Media Breaches
- Procedures for Reporting Testing Incidents
- Test Security Auditor Activities

Purpose and Goal

- By the end of this Webcast, local educational agency (LEA) CAASPP coordinators will be able to train their staff on test security guidelines and procedures for the 2015–16 administration of computer-based tests as well as the paper-pencil tests.

Requirements in the Testing Regulations

Requirements in the Testing Regulations

Test Security Agreement:*

- New form for 2015–16 testing is available.
- Agreement must be read and signed **ANNUALLY.**
- Applies to both computer-based and paper-pencil testing.
- All LEA CAASPP coordinators must electronically submit a signed copy to the California Technical Assistance Center (CalTAC)
  - 100% of all LEAs have already submitted their new signed agreement to CalTAC
- All CAASPP test site coordinators must electronically submit a signed copy of the form; the LEA CAASPP coordinator receives a notification.

* *Pursuant to California Code of Regulations* (*CCR*), Title 5, Section 859(a)

Requirements in the Testing Regulations

Test Security Affidavit:

- New form for 2015–16 is available
- Applies for the 2015–16 school year
- Affidavit must be read and signed **ANNUALLY**
- Applies to both computer-based and paper-pencil testing
- Must be signed by:
  - All test administrators, test examiners, proctors, translators, scribes, LEA CAASPP coordinators, and CAASPP test site coordinators, and any other persons having access to any of the **summative** tests and test materials, assessment technology platform, registration system, or adaptive engine
- LEA CAASPP coordinators keep affidavits on file at the LEA; should not be submitted to CalTAC

* *Pursuant to 5 CCR* Section 859(c)

General Test Security Guidelines

General Test Security Guidelines

- All secure test materials must be handled and stored securely.
  - For computer-based tests, lock any printed rosters in secure storage with limited access; train staff on procedures.
  - For paper-pencil tests, lock in secure storage with limited access; count test booklets upon receipt as well as before and after a testing session; and train staff on the procedures.
- All authorized electronic devices (e.g., assistive device) can be used by students as long as the wireless connectivity has been turned off.
- Seat students so that they cannot easily view each other’s work.

General Test Security Guidelines (cont.)

- Cover or remove materials on the classroom walls that may provide information to students during testing.
- Actively monitor students during testing.
- Report only summative testing incidents using the *STAIRS* form.
- Test administrators and test examiners report to the CAASPP test site coordinator and/or to the LEA CAASPP coordinator.

General Test Security Guidelines (cont.)

- Securely destroy secure test materials that do not need to be returned to Educational Testing Service (ETS).
  - For computer-based summative assessments:
    - Student logon information (tickets)
    - Administrator logon information to the test delivery system
    - Rosters of students scheduled to take the test
    - Scratch paper with students' work
    - Print-on-demand passages, items, and stimulus cards

General Test Security Guidelines (cont.)

- For paper-pencil tests:
  - Test booklets
  - Answer documents (blank with Pre-ID labels and any with student responses recorded)
  - *California Alternate Performance Assessment (CAPA) Examiner's Manuals*
  - *Standards-based Tests in Spanish (STS) Grade 2 Directions for Administration (DFA)*
  - Scratch paper with student's work

General Test Security Guidelines (cont.)

- Printed materials 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.
  - Printed materials from the print-on-demand accommodation
  - Scratch paper
  - Documents with student information
    - Student logon tickets
    - Pre-ID labels

Print-On-Demand Test Security Guidelines

- Test administrators and test examiners are responsible for maintaining the security of printers used for printing CAASPP test content.
  - Before approving or printing an item or stimulus, the test administrator or test examiner must ensure that the printer is on and is monitored by staff.
- Immediately after printing a print-on-demand item/stimulus, the file should be deleted from the test administrator's or test examiner's computer. It must be deleted in such a way that the file does not remain in the "recycle bin" to be undeleted.
  - See page 20 of the *Online Test Administration Manual* for instructions.

Print-On-Demand Test Security Guidelines (cont.)

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

But….

- Scratch paper must be collected after the first part of the Full Write performance task and stored securely until returned to the student during the second part. Scratch paper must be shred according to LEA and/or California policies or procedures after the second part of the Full Write has been completed.

Braille Online Fixed Form

- If a test administrator selects the braille online fixed form (for mathematics only), he or she can pre-order a graphic package that includes pre-embossed graphics to be used while accessing the online fixed form.
- These graphic packages must be ordered through CalTAC and returned to CalTAC after the student has completed testing.

Specific Test Security Guidelines

Preventing Security Violations

- LEA staff, school staff, test administrators and test examiners play a critical role in monitoring the testing session and adhering to directions for standardized administration.
  - Be familiar with test security protocols outlined in the CAASPP Online Test Administration Manual (http://www.caaspp.org/rsc/pdfs/CAASPP.online_tam.2016.pdf)
    - Section 3.0
    - Appendix F

Before and During Testing

- All test items and test materials must remain secure and must be appropriately handled.
  - Includes creating a secure testing environment for what students can see, hear, or access
- The test administrator is ultimately responsible for monitoring and reporting test security issues.
  - Inappropriate Internet access
  - Any other improper display, printing, photographing, duplicating, or sharing of test questions

As Testing Starts and During Testing

- Including first and last name and a picture to logon ticket will help ensure students are logged on to the correct test.
  - Before handing out tickets, use the Test Administrator Interface or the Test Operations Management System to verify that the Statewide Student Identifiers (SSIDs) on the ticket are correct.
- Ensure that students have properly logged on and are taking the test for which they are scheduled.
- Monitor students taking the test for any breach of the secure browser and that it has not allowed students to access external sites or other resources on their testing device during the assessment.

Student Logon for the Computer-based Tests

- Student logon information is considered secure material, so it must be provided to, and viewable only by, the student to whom the logon information pertains.
- Student logon information must be returned to the CAASPP test site coordinator, stored in a secure location between testing sessions, and securely destroyed immediately after testing has been completed.

"(4) (A) I will keep all assigned, generated, or created usernames, passwords, and logins secure and not divulge pupil personal information to anyone other than the pupil to whom the information pertains for the purpose of logging on to the test delivery system." ***CAASPP TEST SECURITY AFFIDAVIT***

"(4) I will securely destroy all print-on-demand papers, scratch paper, and other documents as prescribed within the contractor's(s') or consortium's administrative manuals and documentation." ***CAASPP TEST SECURITY AGREEMENT***

Test Security Guidelines for Computer-based Tests

- Ensure there is adequate space between students so that they cannot see each other’s work.
  - If using a computer lab, consider using temporary dividers (e.g., folders taped to the sides of the monitors).
- Test the equipment and network to be used during testing.
  - Report any workarounds to the secure browser to CalTAC.
  - Some software (e.g., teacher-monitoring software, Apple AirPlay) may need to be disabled or monitored locally.

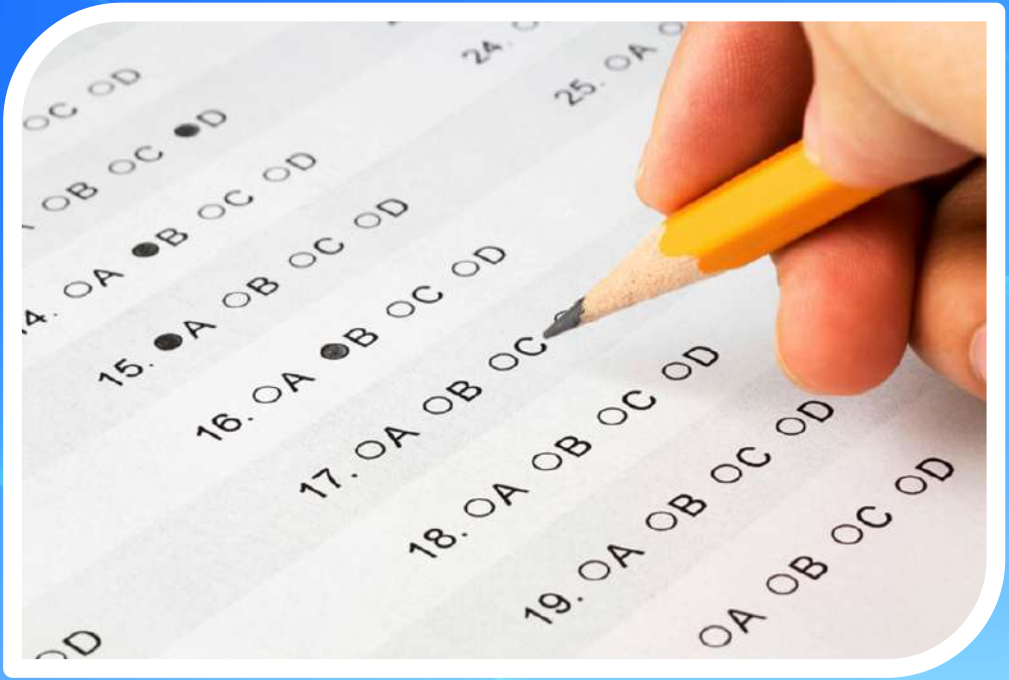
Test Security Guidelines for the Paper-Pencil Tests—Test Administrators and Test Examiners

- Receive and return materials to CAASPP test site coordinator.
- Make sure test booklets and answer documents are distributed to the correct student.
- Allow no unauthorized electronic devices (e.g., cell phones) to be used in classroom during testing.

Test Security Guidelines for the Paper-Pencil Tests—CAASPP Test Site Coordinators

- Before testing: Receive, count, store, and track materials. Materials should be stored in secure storage with limited access, by key or cardkey.
- During testing: Distribute and collect materials from test administrators and test examiners.
- After testing: Count and return materials promptly to the LEA CAASPP coordinator.
- Handle the secure test materials according to the instructions.

Social Media Breaches



Social Media Breaches

- Social media and other Web sites will be monitored daily for postings of secure material.
- A process is in place to ensure the review and investigation of all test security incidents related to social media to determine what action will need to be taken.

Procedures for Reporting Testing Incidents

CAASPP Security and Test Administration Incident Reporting System (STAIRS) Process

- STAIRS and appeals are used for the summative assessments only.
- The online *CAASPP STAIRS* form is the starting point for LEA CAASPP coordinators and CAASPP test site coordinators to report a test security incident or other testing issue that interferes with the administration and completion of the summative assessment.
- Coordinators access the *CAASPP STAIRS* form in the Test Operations Management System by selecting the [**STAIRS/Appeals**] button.
- You cannot submit an appeal request without first submitting the *CAASPP STAIRS* form.
- See *Table 8: Incident types, descriptions, and actions in the CAASPP STAIRS* form starting on page 25 of the *Online Test Administration Manual* for details about incident types and actions.

Procedures for Reporting Testing Incidents—Impropriety

- Unusual circumstance that has a low impact on the testing individual or group of students
- Low risk of affecting student performance, test security, or test validity
- Correctable and containable at local level
- Must be reported to LEA CAASPP coordinator or CAASPP test site coordinator
- **Example:** Students talking during testing

Test Security Chart—Improprieties

None Administration Incident	There is a testing session in which a student deliberately does not attempt to respond appropriately to items.
	A student is unable to complete the test before it expires due to an unanticipated excused absence or unanticipated school closure.
	A student starts a performance task (PT) unintentionally—for example, selects a PT instead of a computer adaptive test, or selects a mathematics PT instead of an English language arts/literacy PT—and the student is unable to complete the test before it expires.
LOW Impropriety	Student(s) making distracting gestures/sounds or talking during the test session that creates a disruption in the test session for other students.
	Student(s) leave the test room without authorization.
	Administrator or coordinator leaving related instructional materials on the walls in the testing room.

Process Flow for Reporting an Impropriety

Procedures for Reporting Testing Incidents—Irregularity

- Unusual circumstance that impacts the testing individual or group of students
- May affect student performance, test security, or test validity
- Correctable and containable at the local level
- **LEA CAASPP coordinator or CAASPP test site coordinator must enter test incident into STAIRS within 24 hours**
  - California regulations require that irregularities be reported to the CDE within 24 hours (5 *CCR* Section 859[e]).
- **Example:** Student accessing or using unauthorized electronic device (e.g., cell phone)

Test Security Chart—Irregularity

MEDIUM Irregularity	Student(s) cheating or providing answers to each other, including passing notes, giving help to other students during testing, or using hand-held electronic devices to exchange information.
	Student(s) accessing the Internet or any unauthorized software or applications during a testing event.
	Student(s) accessing or using unauthorized electronic equipment (e.g., cell phones, PDAs, iPods, or electronic translators) during testing.
	Disruptions to a test session such as a fire drill, school-wide power outage, earthquake, or other acts.
	Administrator or coordinator failing to ensure administration and supervision of the Smarter Balanced assessments by qualified, trained personnel.
	Administrator giving incorrect instructions that are not corrected prior to testing.
	Administrator or coordinator giving out his or her username/password (via e-mail or otherwise), including to other authorized users.
	Administrator allowing students to continue testing beyond the close of the testing window. For the performance task (PT), this is 10 calendar days. For the computer adaptive test (CAT), this is 45 calendar days. For a paper-pencil assessment, this is three weeks.
	Administrator providing a student access to another student’s work/responses (unintentional access granted).
	Student not getting accessibility support or accommodation as required by individualized education program (IEP) or Section 504 plan.

Test Security Chart—Irregularity (cont.)

MEDIUM Irregularity	Student without IEP or Section 504 plan did not get a designated support.
	Administrator or teacher coaching or providing any other type of assistance to students that may affect their responses. This includes both verbal cues (e.g., interpreting, explaining, or paraphrasing the test items or prompts) and nonverbal cues (e.g., voice inflection, pointing, or nodding head) to the correct answer. This also includes leading students through instructional strategies such as think-aloud, asking students to point to the correct answer or otherwise identify the source of their answer, or requiring students to show their work.
	Administrator providing students with nonallowable materials or devices during test administration or allowing inappropriate designated supports and/or accommodations during test administration.
	Administrator allowing designated supports not indicated by an educator (or team of educators with parent/guardian and student input) and that are not in the student's IEP or Section 504 plan.
	Administrator allowing inappropriate accommodations (which are not in the student's IEP or Section 504 plan) during test administration.
	Administrator allowing anyone other than a student to log on to the test unless prescribed as an allowable accommodation in the student’s IEP. This includes test administrators or other staff using student information to log on or allowing a student to log on using another student’s information.
	Administrator providing a student access to another student’s work/responses (intentional access granted).

Process Flow for Reporting a Testing Irregularity

Procedures for Reporting Testing Incidents—Breach

- Event that poses a threat to the validity of the test
- LEA CAASPP coordinator or CAASPP test site coordinator must coordinator must immediately telephone the CDE and then submit a report in STAIRS within 24 hours.
  - California regulations require that irregularities be reported to the CDE within 24 hours (5 *CCR* Section 859[e]).
- **Example:** Release of secure materials or a security/ system risk
- Circumstances have an external implication to the Smarter Balanced Assessment Consortium
  - May result in decision to remove an item from scoring

Test Security Chart—Breach

HIGH BREACH	Administrator or coordinator modifying student responses or records at any time.
	The live Student Interface or Test Administrator Interface being used for practice instead of the training or practice tests.
	Adult or student posting items or test materials on social media (Twitter, Facebook, etc.).
	Administrator allowing students to take home printed test items, reading passages, writing prompts, or scratch paper that was used during the test or failing to otherwise securely store test materials.
	Adult or student copying, discussing, or otherwise retaining test items, reading passages, writing prompts, or answers for any reason. This includes the use of photocopiers or digital, electronic, or manual devices to record or communicate a test item. This also includes using secure test items, modified secure test items, reading passages, writing prompts, or answer keys for instructional purposes.
	Secure test materials being shared with the media (such as the writing prompts, test items, or reading passages), or allowing media to observe a secure test administration.
	Adult or student improperly removing secure testing materials such as test items, stimuli, reading passages, writing prompts, or scratch paper from the testing environment.
	Lost or missing student logon information.

Process Flow for Reporting a Testing Breach

Measuring the Power of Learning.™

Test Security Webcast: STAIRS Live Demo

Chang Yi

ETS

3/09/16

Test Security Auditor Activities

Test Security Audits

- Audits are conducted throughout the state.
- Auditors will:
  - observe test security processes being used.
  - interview the CAASPP test site coordinator or designee before, during, and after testing.
- Summary reports will be provided to the CDE and will be shared with the LEA CAASPP coordinator.

Questions

Help Desk Support

- The CalTAC is there to support all LEA CAASPP Coordinators!

Available Monday – Friday from 7 a.m.– 5 p.m. PT

E-mail: caltac@ets.org

Phone: 800-955-2954

Web site: http://www.caaspp.org/