

General Test Security Guidelines



General Test Security Guidelines

- All secure test materials must be handled and stored securely.
 - For paper-pencil tests, lock in secure storage with limited access; count test booklets before and after a testing session; and train staff on the procedures.
 - For computer-based tests; lock any printed rosters in secure storage with limited access; train staff on procedures.
- The use of unauthorized electronic devices (e.g., cell phones) in the testing session is prohibited.
- Seat students so that they cannot easily view each other's work.

General Test Security Guidelines

- Cover or remove materials on the classroom walls that may provide information to students during testing.
- Actively monitor students during testing.
- Securely destroy secure test materials that do not need to be returned to the Educational Testing Service (ETS).
- Report irregularities and improprieties.
 - Test administrators (TAs) report to the CAASPP Test Site Coordinator and/or to the LEA CAASPP Coordinator.

General Test Security Guidelines

- What are secure test materials?
 - 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

- What are secure test materials? (continued)
 - For computer-based tests:
 - Student logon information
 - Administrator logon information to the Test Delivery System
 - Rosters of students scheduled to take the test
 - Scratch paper with students' work
 - The Smarter Balanced items
 - Passages, items, and stimulus cards printed on demand

Print-On-Demand Test Security Guidelines

- Before the TA approves the student's request to print a test item/stimulus, the TA 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 Administrators computer. It must be deleted in such a way that the file doesn't remain in the "recycle bin" to be undeleted.

Print-On-Demand Test Security Guidelines

- Printed materials from the print-on-demand accommodation 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.

Print-On-Demand Test Security Guidelines

- 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 immediately shredded according to LEA and/or California policies or procedures.

Test Security Guidelines for Computer-based Tests



Preventing Security Violations

- LEA staff, school staff, and TAs 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 (TAM)
 - Section 3.0
 - Appendix C

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 TA 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

- 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 Login for the Computer-based Tests

- Student login information is considered secure material, so it must be provided to, and viewable only by, the student to whom the login information pertains.
- Student login information must be returned to the CAASPP Test Site Coordinator, stored in a secure location between testing sessions, and securely destroyed immediately after testing.

“(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 assessment 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 the CDE and CalTAC.
 - Some software (e.g., teacher-monitoring software, Apple AirPlay) may need to be disabled or monitored locally.