

NH Smarter Balanced Test Security Summary Document

This document is supplemental to security instructions contained in Smarter Balanced Manuals and Guides located on the New Hampshire SBAC Portal at <http://nh.portal.airast.org/>

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.

Violation of test security is a serious matter with far-reaching consequences. Breaches of test security include, but are not limited to copying of test materials, failing to return test materials, coaching students, giving students answers, and/or changing students' answers. Such acts may lead to the invalidation of an entire school district's student test scores, disruption of the test system statewide, and legal action against the individual(s) committing the breach. A breach of test security may be dealt with as a violation of Professional Responsibility for Teachers, as well as a violation of other pertinent state and federal law and regulations. The New Hampshire State Department of Education will investigate all such matters and pursue appropriate follow-up action. Any person found to have intentionally breached the security of the test system may be subject to sanctions including, but not limited to, disciplinary action by a local board of education, the revocation of New Hampshire teaching certification by the State Board of Education, and civil liability pursuant to federal copyright law.

Plans supporting adequate training on test security procedures for Test Administrators, Test Coordinators, Test Proctors, and any individuals supporting test administration should be on file with each educational facility. Such training should include, but not be limited to, training on item security, adherence to *Online Test Administrator Manual* policies.

With regard to overall test security, the New Hampshire Department of Education recommends that each Local Education Agency have in place a process and associated timeline for ensuring that:

- Test Administrators (and any other individuals who will be administering any secure Smarter Balanced assessments) have read and understand the Smarter Balanced *Online TAM*, the Smarter Balanced *Usability, Accessibility, and Accommodations Guidelines*, and associated Smarter Balanced training modules.
- There are clearly defined protocols that describe which individuals (staff or otherwise) may be designated as Test Administrators or in other roles related to administering a secure Smarter Balanced assessment.
- There is a process in place for monitoring social media for the posting of any secure assessment materials.

Breaches must be reported to Smarter Balanced immediately and irregularities must be reported by the end of the day of the incident to the state via telephone followed by the Test Security Incident Log.

RESPONDING TO TESTING IMPROPRIETIES, IRREGULARITIES, AND BREACHES

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 rules, either by staff or students, constitutes a test security incident. Improprieties, irregularities, and breaches need to be reported in accordance with the following instructions.

The information in the following table is provided to assist you in determining the level of security incidents.

This list is not intended to include every possible circumstance where a security breach might occur.

Impact and Definitions

Definitions for Test Security Incidents Type	Definition
Impropiety	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, test security, or test validity. These circumstances can be corrected and contained at the local level. An impropriety should be reported to the District Test Coordinator (DC) and School Test Coordinator (SC) immediately and entered in the TIDE system as necessary (should an appeal be required).
Irregularity	An unusual circumstance that impacts an individual or group of students who are testing and may potentially affect student performance on the test, test security, or test validity. These circumstances can be corrected and contained at the local level and submitted in the online appeals system for resolution. An irregularity must be reported to the DC and SC immediately and entered in TIDE within 24 hours of the incident (should an appeal be required).
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/system risk. These circumstances have external implications for the Consortium 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 DC and SC immediately and entered in TIDE (should an appeal be required).

Reporting Timelines and Activities

- **Improprieties** are escalated in accordance with state policies and procedures, protocols, and/or guidelines within 24 hours of the incident by individual districts via the Test Security Log or other mechanism as designed by the State and via the TIDE Appeals system where appropriate.
- **Irregularities** must be escalated by the end of the day of the incident to the state level via the Test Security Incident Log or other mechanism as designed by the State and via the TIDE Appeals system where appropriate.
- A **Breach** requires immediate notification/escalation by telephone to the state level by the DC, followed by documentation in the Test Security Incident Log.

Test Security 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, has a low risk of potentially affecting student performance on the test, on test security, or in test validity. (Example: Student(s) leaving the testing room without authorization.)

- Local administrators/ staff take corrective action and document impropriety in Test Security Incident Log.
- Incident is mitigated as necessary by school staff, and DC is notified for assistance with mitigation as necessary.
- Designated district employee (such as SC/DC) records impropriety via log or TIDE (if appropriate) within 24 hours.
- State authorizes TIDE appeal (if appropriate).

Irregularity

An unusual circumstance that impacts an individual or group of students who are testing and may potentially affect student performance on the test, test security, or test validity. These circumstances can be contained at the local level. (Example: Disruption during the test session such as a fire drill.)

- Local administrators/staff take corrective action and document impropriety in Test Security Incident Log.
- Incident is mitigated as necessary by school staff, and DC is notified for assistance with mitigation.
- Designated district employee (such as SC/DC) escalates irregularity via log or in TIDE (if appropriate) by the end of the day of the incident.
- State reviews TIDE record of irregularity in accordance with state protocol.
- State employee authorizes TIDE appeal.

Breach

Any test administration event that poses a threat to the validity of the test. Breaches require immediate attention and escalation to the state agency. Examples may include such situations as exposure of secure materials or a repeatable security/system risk. These circumstances have external implications. (Example: Administrators modifying student answers, or test items shared in social media.) All breaches in test administration are handled at multiple levels.

Local Level

- Local administrators/ staff report breach to SC and/or DC immediately.
- Local administrators/ staff contain the incident as necessary.
- Local administrators/ staff document incident in local Test Security Incident log and in TIDE (if appropriate).
- Local administrators/ staff stand ready to receive further State guidance on dispensation of event.

District Level

- District staff investigate security risk and alert State Leads via phone.
- District staff verify completion and accuracy of Test Security Incident Log.
- District staff maintain communication with school and provide guidance as appropriate.

State Level

- State employee reviews incident and containment strategies employed by the district and authorizes TIDE appeal as necessary.
- State stands ready to receive further Consortium guidance.

The Test Security Incident Log is the document of record for all test security incidents and should be maintained at the district level. More serious incidents will be reported either immediately (breach) or at the end of the day (irregularity).

Documentation of Security Incidents: Use of Incident Log and Appeals System
School and District Test Coordinators should ensure that all test security incidents are documented in a Test Security Incident Log.

The Test Security Incident Log is located on the NH DOE Assessment Page. TAs must download the template and log incidents immediately upon identification and submit them, via email or alternate agreed-upon process, to their SCs and DCs. District staff should establish a process that includes how frequently these logs should be submitted and communicate this preference to schools. The description of each column header is included in the template. In addition to logging all test security incidents in the Test Security Incident Log, incidents requiring specific

actions to be taken regarding the test itself are to be escalated—following the procedures noted in the previous section.

Test Security Chart shows the test security incident levels and examples of types of issues.

The information in the following table is provided to assist you in determining the level of security incidents.

This list is not intended to include every possible circumstance where a security breach might occur.

Level of Severity and Potential Effect on Test Security	Types of Issues
LOW Impropriety	<p>Student(s) making distracting gestures/sounds or talking during the test session that creates a disruption in the test session for other students.</p> <p>Student(s) leave the test room without authorization.</p> <p>Testing staff leaving related instructional materials on the walls in the testing room.</p>
MEDIUM Irregularity	<p>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.</p> <p>Student(s) accessing the Internet or any unauthorized software or applications during a testing event.</p> <p>Student(s) accessing or using unauthorized electronic equipment (e.g., cell phones, iPods, or electronic translators) during testing.</p> <p>Disruptions to a test session such as a fire drill, school-wide power outage, or other acts.</p> <p>Testing staff giving incorrect instructions that are not corrected prior to testing.</p> <p>Testing staff giving out his or her username/password (via email or otherwise), including to other authorized users.</p> <p>Testing staff 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.</p> <p>Testing staff providing students with non-allowable materials or devices during test administration or allowing inappropriate designated supports and/or accommodations during test administration.</p> <p>Testing staff providing a student access to another student’s work/responses.</p>
HIGH Breach	<p>Testing staff modifying student responses</p> <p>The live Student Interface or TA Interface being used for practice instead of a live test administration. Live interfaces should only be accessed via the secure browser for live Smarter Balanced Assessments. Any practice or training tests should be taken on the Practice Test and Training Test sites, located on the portal.</p> <p>Testing staff allowing students to take home printed test items, reading passages,</p>

	<p>writing prompts, or scratch paper that was used during the test or failing to otherwise securely store test materials.</p> <p>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.</p> <p>Secure test materials (e.g., writing prompts, test items, or reading passages) being shared with the media, or allowing media to observe a secure test administration.</p> <p>Adult or student improperly removing secure testing materials, such as test items, stimuli, reading passages, writing prompts, or scratch paper from the testing environment.</p>
--	--

Assessment security measures must be adhered to before, during, and after testing in order to ensure the validity, reliability and fairness of the assessment results. Tests must be administered strictly in accordance with the instructions and procedures set forth in the test administration manuals and assessment security instructions and procedures provided by the Smarter Balanced Assessment Consortium.

Pursuant to Ed. 306.24:C (2) "Procedures for test security and the accurate inclusion of student data;" All New Hampshire schools should have process and procedure in place and an associated timeline for ensuring that Test Administrators, Coordinators, Proctors (and any other individuals who will be administering any secure assessment) have read and understand all test administration materials, information and forms associated with Smarter Balanced assessments. Schools and districts should also have a process in place for monitoring social media for the posting or discussion of any secure assessment items and/or materials. All improprieties, irregularities and breaches should be recorded on the appropriate Test Security Log sheet and reported to the New Hampshire Department of Education.

The information in the following table is provided to assist you in determining what activity might constitute a breach of security. This list is not intended to include every possible circumstance where a security breach might occur.

All persons are prohibited from providing students with the answers to test items or inquiry tasks at any time (before, during, and after test administration has been completed). This includes provision of cues, clues, hints and/or actual answers in any written, printed, electronic, verbal and/or non-verbal form.	
Use of secure test materials at times, and for purposes other than those approved by the New Hampshire Department of Education is strictly prohibited .	
BEFORE TESTING	
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).

NH SBAC Test Security Summary

Student seating	Students must be seated so there is enough space between them to minimize opportunities to look at each other's work.
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.
DURING TESTING	
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 must be actively monitored and are prohibited from access to unauthorized electronic devices that allow availability to outside information, communication among students, or photographing or copying test content. This includes any device with cellular, messaging, or wireless capabilities, but is not limited to cell phones, iPods, cameras, and electronic translation devices.
Access to allowable resources only	Students must only have access to and use of those allowable resources that are permitted for each specific test (or portion of a test).
Allowable Accommodations	Allowable testing accommodations remove barriers to participation so that these students may provide their own responses without giving them an advantage over other students.
Access to assessments	Only students who are testing can view items. Students who are not being tested or unauthorized staff or other adults must not be in the room where a test is being administered. Trained Teachers and Test Administrators may have limited exposure to items in the course of properly administering the assessments; however, DCs, SCs, TEs and TAs, and other trained staff may not actively review or analyze any items.
No answer key development	No form or type of answer key may be developed for test items.
Using Test Items	Using test items and inquiry tasks in <u>any</u> form (including rewording actual test items) during the testing process is strictly prohibited .
Monitor Testing	During the test administration, Test Administrators should monitor the testing process by moving unobtrusively about the room. It is difficult to observe testing in progress if one merely sits or stands in the front of the room. The Test Administrator is to devote <u>total attention</u> to the students being tested and to avoid involvement in paperwork or any other activity that distracts from actively proctoring the test.
DURING AND AFTER TESTING	
No access to responses	DCs, SCs, TAs, TEs, and other staff are not permitted to review student responses or students' notes on scratch

NH SBAC Test Security Summary

	paper.
No copies of test materials	No copies of the test items or materials 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 or materials. Similarly, these materials must not be discussed with or released to anyone via any media, including fax, e-mail, social media websites, etc.
No retaining, discussing, or releasing test materials	Descriptions of test items or materials must not be retained, discussed, or released to anyone.
No reviewing, discussing, or analyzing test materials	DCs, SCs, TAs, TEs, and other staff may not review, discuss, or analyze test items or materials at any time, including before, during, or after testing. Student interaction during a test is limited to what is necessary for the purpose of the Classroom Activity.
Prohibited from changing or editing student work	Responses to test items and performance tasks must represent the student’s own independent and unaided thinking and must remain unchanged after test administration is complete. All persons are prohibited from changing or editing students’ answers to test items or performance tasks, either by providing hints or clues to wrong answers during test administration or by correcting wrong answers recorded, or provided in other ways, by the student.
All test materials must be kept secure	All test materials, scratch paper, and documents with student information must be kept in a securely locked location.