

Procedures for Investigating Cell Phone Violations

During statewide testing, students are not permitted to use, or be in possession of any electronic device (e.g., cell phone, smartphone/watch camera, PDA, or playback device, etc.) that could allow them to view, access, retain, or transmit information for any state-mandated assessment. Students who use an electronic device for medical purposes (e.g., glucose monitoring, cardiac monitoring) may be allowed access to the device(s) during testing.

Districts and schools must have a plan to collect and secure prohibited devices so that they are not accessible during testing. In the event a student fails to follow instructions for prohibited devices but **does not use it during testing**, the TA and/or monitor must collect the device if they become aware of its presence and should allow the student to continue testing. Enforce appropriate district and/or school disciplinary policies for this type of incident.

Cell Phone/Electronic Device Use Reported During Testing

If a TA, monitor or STC discovers that **a student or students were using a cell phone** or other electronic device during a test, the following general procedures should be followed.

If a student is viewed with or using a cell phone or another electronic device during testing, the TA or STC must:

1. Collect the cell phone or electronic device from the student.
2. Stop testing the student and remove the student from the classroom following the test security guidelines developed by the school or district.
3. Notify the principal and the STC. The STC must notify the DTC.
4. The DTC must notify the Office of Assessment and Standards (OAS) that a test security violation (TSV) occurred using a cell phone or other electronic device.
5. A school or district IT staff person, or another educator who is experienced/knowledgeable with the type of device and applications, must conduct a reasonable search of the cell phone/electronic device. The search would include:
 - a. accessing open applications, text messages/various messaging apps (e.g., Messenger, WhatsApp, etc.);
 - b. accessing social media sites (e.g., SnapChat, Instagram, TikTok, etc.);
 - c. looking for recent, deleted, and hidden photos;
 - d. searching for other electronic communications and support applications (e.g., Notes, Translate, Google Photos, Google Drive, Dropbox, Photomath, CyMath, etc.);
 - e. searching recent history on web browsers (e.g., Chrome, Safari, Firefox, etc.) noting that there may be more than one browser on the device;
 - f. checking for multiple student profiles — students may have one profile their parents monitor and another profile the parent(s) do not know about; and,
 - g. checking for discussions of items, pictures of the class, images of test forms, test items, answers to item questions, or anything associated with testing.
6. STCs and/or DTCs must document the prohibited messages, texts, or images found on the cell phone and provide the photos, screen shots, messages, etc. to the OAS.
7. STCs and DTCs must follow the procedures outlined in the TAM for investigating/reporting a TSV.

Cell Phone/Electronic Device Use Reported (Suspected) After Test Session Completed

If the TA, STC or other educator learns that a cell phone test security violation is suspected, but not yet confirmed, the STC must ask the student(s) to turn in the cell phone(s) for examination.

If the student complies:

1. Notify the principal and the STC. The STC must notify the DTC.
2. Notify the Office of Assessment and Standards (OAS) that a *possible* test security violation (TSV) has occurred using a cell phone or other electronic device.
3. Begin a thorough investigation of the circumstances surrounding the incident. The student may need to provide any password, facial recognition, or biometric-protected data to open the cell phone or electronic device. Failure to provide any password, etc. may automatically lead to invalidating the test score.
4. STCs and/or DTCs must interview the student and notify the student's parent or guardian.
5. A school or district IT staff person, or another educator who is experienced/knowledgeable of the type of device and applications, must conduct a reasonable search of the cell phone/electronic device. The search would include:
 - a. accessing open applications, text messages/various messaging apps (e.g., Messenger, WhatsApp, etc.);
 - b. accessing social media sites (e.g., SnapChat, Instagram, TikTok, etc.);
 - c. looking for recent, deleted, and hidden photographs;
 - d. searching for other electronic communications and support applications (e.g., Notes, Translate, Google Photos, Google Drive, Dropbox, Photomath, CyMath, etc.);
 - e. searching recent history on web browsers (e.g., Chrome, Safari, Firefox, etc.) noting that there may be more than one browser on the device;
 - f. checking for multiple student profiles - students may have one profile their parents monitor and another profile the parent(s) do not know about; and,
 - g. checking for discussions of items, pictures of the class, images of test forms, test items, answers to item questions, or anything associated with testing.
6. STCs and/or DTCs must document the prohibited messages, texts, or images found on the cell phone and provide the photos, screen shots, messages to the OAS.
7. If cheating or test exposure occurred, invalidate the student's test. Enforce any additional school/district policies on cheating such as suspension or other disciplinary actions as outlined in the district discipline policy.
8. STCs and DTCs must follow the procedures outlined in the TAM for investigating a TSV.

If the student does not comply to the request to provide the cell phone:

1. Interview the student and notify the student's parents or guardians.
2. Begin a thorough investigation of the circumstances surrounding the incident.
3. Notify the Office of Assessment and Standards (OAS) that a *possible* test security violation occurred using a cell phone or other electronic device.

4. Contact the local police regarding the test security incident requesting that the phone/device in question be secured from the student. If needed, the district should read or send a copy of the test security laws and regulations to the police representative. The police or the school/district may analyze the cell phone or electronic device for theft of test content.
5. If the police department secures the cell phone or electric device, the school/district may conduct the forensic analysis of the phone or someone in the police department may be asked to examine the phone for illegal test content.
6. A reasonable search of the cell phone/electronic device must be conducted. The search would include:
 - a. accessing open applications, text messages/various messaging apps (e.g., Messenger, WhatsApp, etc.);
 - b. accessing social media sites (e.g., SnapChat, Instagram, TikTok, etc.);
 - c. looking for recent, deleted, and hidden photographs;
 - d. searching for other electronic communications and support applications (e.g., Notes, Translate, Google Photos, Google Drive, Dropbox, Photomath, CyMath, etc.);
 - e. searching recent history on web browsers (e.g., Chrome, Safari, Firefox, etc.) noting that there may be more than one browser on the device;
 - f. checking for multiple student profiles - students may have one profile their parents monitor and another profile the parent(s) do not know about; and,
 - g. checking for discussions of items, pictures of the class, images of test forms, test items, answers to item questions, or anything associated with testing.
7. STCs and/or DTCs must document the prohibited messages, texts, or images found on the cell phone and provide the photos, screen shots, messages to the OAS.
8. If cheating or test exposure occurred, invalidate the student's test. Enforce any additional school/district policies on cheating such as suspension or other disciplinary actions as outlined in the district discipline policy.
9. STCs and DTCs must follow the procedures outlined in the TAM for investigating/reporting a TSV.