

Test Security Protocol

Delaware Christian School



Test security is vital to the successful administration of state assessments for many reasons, such as:

- Ensuring student results are accurate and meaningful;
- Maintaining confidentiality of tests;
- Safeguarding the investment of resources, time and effort required to develop assessments at the school, district and state levels;
- Avoiding investigations, invalidations or disciplinary actions; and
- Providing accurate measures for use in accountability.

Secure test materials include, but are not limited to, blueprints; test layout forms; item pools; operational and field test books, answer keys, and test questions, or test book sections. Secure test materials may be in either electronic or paper format. To comply with Ohio Department of Education's regulation on the ensurement of test security, Delaware Christian School agrees to enforce the following policies:

Authorized Personnel

Only authorized personnel will handle secure test materials. Authorized Personnel include:

- District Test Coordinator
- Test Administrator (Teacher administering the test)
- Office Administrator responsible for locking and unlocking any secure test materials

Handling Test Materials

Testing materials will be kept in a locked file cabinet. All test materials will be handled by the test coordinator, or in her absence, whomever she designates. All test materials will be signed out and signed in immediately before and after administering the test. Only authorized personnel may check in or check out test materials. Students are not allowed to handle

secure test materials for any reason other than to take their individual test during the test period.

No person shall reveal, cause to be revealed, release, cause to be released, reproduce, or cause to be reproduced any secure assessment materials through any means or medium including, but not limited to, electronic, photographic, photocopy, written, paraphrase, or oral.

Investigating Alleged Security Violation

DCS authorizes the right to investigate any alleged security violation including but not limited to illegal device usage during a test session, cheating, distribution of test items.

Electronic Device Policy

Electronic devices include but are not limited to cell phones, smartwatches and other WIFI-enabled, non-testing devices. High School students are expected to turn off and lock all electronic devices in DCS issued Yonder pouches and are to be left in the student's assigned locker for the duration of the testing period. Middle school students are expected to turn off and lock all electronic devices in DCS issued Yonder pouches which are then collected by a staff member. Elementary school students are expected to turn off and leave all electronic devices in their assigned locker for the duration of the testing period. Any electronic device in a testing room, even after a student has completed testing, has the potential to be a test security violation. In the absence of a school issued accommodation, listening to music while actively testing will not be permitted. Any violation will be subject to the school's policy on inappropriate technology use in the classroom. **Accessing an electronic device during testing can be grounds for an invalidation.** If cheating can be ruled out, DCS may elect not to invalidate the test and the student can continue testing based on the severity of the infraction.

If a student is observed using a cell phone or other Wi-Fi enabled device during or after the test session, DCS staff will investigate if any test question, passage or prompt was photographed, texted, shared with anyone at any time or in any way compromised. In extreme cases where test questions, passages or prompts were posted on any social medium, Ohio State Testing Administration will be immediately contacted. These are test security violations. The student's test opportunity is over and the test must

be invalidated.

Students who use an electronic device for medical purposes (for example, glucose monitoring or hearing aid) may have access to the device during testing. The device should only support the student for medical reasons and the test administrator must closely monitor the use of the device to maintain test security during testing.

Test administrators may have a cell phone or other Wi-Fi enabled device for medical and technological emergencies, to use as a time keeper or to otherwise perform necessary test-related actions. **Test administrators must not use these devices for non-test related activities or for personal use.** Test administrators should never take photographs of students, tests, computer screens or the testing room during testing.

Social Media

Sharing an image of a test item or a description in words on any social media is a test security violation and identified as cheating. All students deserve a fair testing experience. Sharing images of test items via Twitter, Instagram, Snapchat, Facebook or other social media sites – or posting a description of or basic information about test items – results in an unfair test environment by providing some students and teachers with advanced information about test questions. This creates an uneven playing field and gives some students an advantage over others and impairs the ability of schools to get valuable information about how their students are performing. Also, when test items are compromised, they must be replaced at the expense of Ohio taxpayers.

A test item posted to social media sites or elsewhere on the internet is a test security violation. Social media and other web pages often include information that indicates the name and location of the person who posted the live test item. **The test for the student who posted the secure material will be invalidated and no breach form will be allowed.** DCS will conduct an investigation to determine if the test administrator was actively monitoring the testing session.