

Blanchester Local School District



2026-27 Test Security Plan

Blanchester Local School District

Test Security Plan 2026–2027

Effective Dates: 2026–2027 Academic Year

Scope: District-Wide (Blanchester High School, Blanchester Middle School, Putman Elementary)

Target Audience: District & Building Test Coordinators, Administrators, Test Administrators, Technology Staff, and Support Personnel

1. Statutory and Regulatory Authority

The Blanchester Local School District (BLSD) Test Security Plan is established in strict alignment with Ohio Revised Code (ORC) and Ohio Administrative Code (OAC) regulations established by the Ohio Department of Education and Workforce (ODEW). Compliance with these standards is mandatory for all district personnel involved in the preparation, administration, scoring, or handling of state-mandated assessments.

- [**ORC Section 3319.151**](#): Prohibits revealing test questions, assisting students in cheating, violating security procedures, or compromising the integrity of state assessments. Violation of this section may lead to civil action, loss of educator licensure, and disciplinary action up to termination.
- [**OAC Rule 3301-13-02**](#): Administering State Tests—Outlines rules for test windows, student participation, and required testing accommodations.
- [**OAC Rule 3301-13-05**](#): Establishing Security and Security Investigation Provisions for Tests—Mandates district security procedures, handling of secure materials, reporting of security breaches, and invalidation protocols.
- [**OAC Rule 3301-7-01**](#): Standards for the Ethical Use of Tests—Establishes professional ethical standards regarding test preparation, administration, and reporting.
- [Blanchester Local Schools Cell Phone Policy](#)
- [Blanchester Local Schools AI Policy](#)

2. Roles and Responsibilities

Role	Key Responsibilities
District Test Coordinator (DTC)	Oversees district-wide test security, manages system access in TIDE/Assessment System, conducts mandatory annual security training, distributes and collects secure materials, investigates reported security breaches, and submits formal invalidations and reports to ODEW.
Building Test Coordinator (BTC)	Manages building-level test scheduling, maintains locked chain-of-custody storage, issues and collects secure test tickets and materials daily, oversees active monitoring in rooms, submits student rosters to DTC, and immediately reports potential security incidents to the DTC.

Role	Key Responsibilities
Test Administrator (TA)	Licensed educators who complete annual test security training, actively monitor students during testing sessions, enforce non-testing device prohibitions, verify accommodations, and log chain-of-custody handoffs.
Technology Coordinator	Ensures secure browser installation on all student testing devices, configures network security, manages device locking features, and provides immediate technical support during testing windows.

3. Annual Staff Training & Ethical Use Standards

In accordance with state guidelines, all staff participating in state testing must undergo mandatory security training prior to the administration of any state assessment.

- **Annual Training Requirement:** All DTCs, BTCs, TAs, and hallway/proctor monitors must complete annual test security training prior to the start of the testing window. Training documentation and signed agreement forms are maintained by the DTC for three (3) years.
- **Annual Parent & Student Notification:** District security policies, including electronic device rules and consequences for cheating, are published and distributed annually in writing before October 1.
- **Ethical Preparation:** Teachers may prepare students using ODEW-released items and practice tests. Drill-and-kill practices using actual or recreated secure test items, coaching students during testing, or editing/altering student responses are strictly illegal and unethical.

4. Chain of Custody & Secure Storage Protocols

Maintaining a complete, documented chain of custody for all physical and digital assessment materials is required at all times.

- **Secure Storage Facility:** All physical secure materials (Student Testing Tickets, testing rosters, paper test booklets, answer documents, special accommodations materials) must be stored in a central, doubly locked secure room or locked safe. Access is restricted exclusively to designated Test Coordinators.
- **Daily Log Tracking:** TAs must sign out secure materials (including Student Testing Tickets and formula sheets) immediately prior to the test session and return/sign them back in immediately following the session.
- **Scratch Paper & Working Materials:** Used scratch paper, graph paper, and student notes are considered secure materials. All used scratch paper must be collected immediately after testing, inventoried, and kept in locked storage until securely shredded. Shredding logs must be retained for three (3) years. [Materials Shredding Document](#)
- **Post-Test Certification:** Upon conclusion of each testing window, BTCs must complete and submit a signed Post-Test Certification Form verifying that all secure materials have been accounted for and returned or destroyed according to state protocol.

5. Electronic Device, Artificial Intelligence, and Social Media Policies

To protect test content integrity in modern digital environments, strict electronic device rules apply to all students and staff.

- **Student Non-Testing Devices:** Cell phones, smartwatches, fitness trackers, Bluetooth headphones, e-readers, tablets, and personal laptops are strictly prohibited in the testing room. Devices must be powered off and stored in locker facilities or designated collection bins away from testing desks.
 - [Cell Phone Policy](#)
- **Artificial Intelligence (AI) Prohibition:** Capturing images or text of test questions to submit to AI tools (e.g., ChatGPT, Claude, Gemini, Photomath) is a critical security violation resulting in immediate test invalidation and disciplinary action.
 - [AI Policy](#)
- **Social Media Violations:** Posting photos, descriptions, or commentary regarding secure test content on social media platforms (such as X, Instagram, Snapchat, TikTok, or Facebook) constitutes severe cheating. If a student posts content to social media, both parts/sessions of the test subject must be invalidated immediately without eligibility for a breach form reset.
- **Test Administrator Devices:** TAs are permitted to carry a device solely for official emergency communication, timekeeping, or technical assistance. TAs are strictly forbidden from taking photographs of students, test screens, or room setups, or using devices for personal reasons during active testing.
- **Building Security Cameras:** Building security cameras situated in testing rooms may remain powered on, provided they do not zoom in or capture legible details of student testing screens or secure paper materials.

6. Active Monitoring Guidelines

Active monitoring is required throughout every test session to guarantee a standardized, secure testing environment.

- **Continuous Movement & Observation:** TAs must continuously walk around the room to observe student engagement, verify students are working in the correct test unit, and ensure prohibited devices are not in use.
- **Prohibited TA Conduct:** TAs may not read books, grade papers, use mobile phones for personal business, work on computers, or engage in conversations that distract testing students.
- **Student Assistance Rules:** TAs MUST NOT read passages/questions (unless designated by an IEP/504 read-aloud accommodation), explain word meanings, rephrase questions, or give any direct or indirect feedback regarding student answers.

7. Security Breaches, Investigations, and Invalidation Procedures

Any suspected or observed violation of test security protocols must be reported immediately to ensure rapid investigation and compliance with state reporting rules.

- **Immediate Reporting:** Staff members who observe a potential breach (e.g., cell phone

usage, student cheating, unauthorized assistance, missing testing tickets) must notify the BTC and DTC immediately.

- **Investigation Protocol:** The DTC will initiate a formal investigation, including collecting written statements from involved staff and students, gathering physical evidence, and conducting interviews.
 - [Investigation Report](#)
- **Corrective Action & ODEW Reporting:** When required by OAC 3301-13-05, the DTC will submit a formal written inquiry report and Corrective Action Plan to the Ohio Department of Education and Workforce (ODEW) Office of Assessment.
- **Test Invalidations:** Test invalidations must be officially requested and processed in the Assessment System by the DTC. Reasons for invalidation (e.g., student illness, cheating, device violation) must be documented in district records.

Test Security Violations

The following lists describe various security violations (actions prohibited before, during, and after testing that compromise test security) regarding electronic devices, test supervision, and test materials. These lists are intended as examples only and are not comprehensive. Test Administrators reserve the right to add security violations to the following lists at their discretion.

Examples of Test Security Violations - *Electronic Devices*

- Using a cell phone or other prohibited handheld electronic device (e.g., smartphone, iPod®) while secure test materials are still distributed or while students are testing. (Exception: Test Coordinators, Technology Coordinators, Test Administrators, and Proctors are permitted to use cell phones in the testing environment only in cases of emergencies or when timely administration assistance is needed. LEAs may set additional restrictions on allowable devices as needed.)
- Technology Coordinators may NOT take photos of testing screens.
- Listening to music on a device or through headphones while secure test materials are still distributed or while students are testing.
- Using a computer, laptop, or tablet (other than the one being used to administer a computer-based test) while secure test materials are still distributed or while students are testing.

Examples of Test Security Violations - *Test Supervision*

- Explaining passages or test items to students.
- Coaching students during testing, including giving students verbal or nonverbal cues, hints, suggestions, or paraphrasing or defining any part of the test.
- Engaging in activities that prevent proper student supervision at all times while secure test materials are still distributed or while students are testing (e.g., grading papers, reading a book, newspaper or magazine).
- Leaving students unattended for any period of time while secure test materials are still distributed or while students are testing.
- Giving students more or less time than is allotted for the test as outlined in the manual (except for students who have the extended time accommodation specified in an approved IEP, 504 Plan, or, if required by your state, an EL Plan).
- Encouraging students to finish early.

- Allowing students to pass notes, talk, or cause disturbances while test materials are still being distributed or while students are testing.
- Providing unauthorized persons with access to secure materials.
- Formally or informally scoring student responses to test items.
- Allowing students to test before or after your state's test administration window.

Examples of Test Security Violations - *Test Materials*

- Leaving test materials unattended or failing to keep test materials secure at all times while secure test materials are still distributed or while students are testing.
- Viewing or permitting students to view secure test content at any time other than during testing.
- Reading or viewing the passages or test items before, during, or after testing.
(Exception: In special cases where a Test Administrator reads aloud to a student (human reader or human signer). Reading to a student who meets the requirements and has the Human Reader accommodation listed in his or her IEP or 504 Plan is permitted)
- Copying or reproducing (e.g., taking a picture of) any part of the passages or test items or any secure test materials or online test forms.
- Altering or interfering with a student's responses in any way.
- Making responses available to a student.
- Handling the test materials for a purpose other than test administration (e.g., teacher takes a Test Booklet home to review, Test Administrator reads a student's responses after school).
- Revealing or discussing passages or test items with anyone, including students and school staff, through verbal exchange, email, social media, or any other form of communication.
- Removing secure test materials from the school's campus or removing them from locked storage for any purpose other than administering the test

Testing Irregularities

The following lists describe testing irregularities (i.e., actions or events that may occur before, during, or after administration that may compromise the validity of the test) regarding the testing environment and testing procedures. These are intended as examples only and are not comprehensive. Test Administrators reserve the right to add testing irregularities to the following lists at their discretion.

Examples of Testing Irregularities - *Testing Environment*

- Building evacuation or lockdown.
- Unauthorized visitors in the testing environment.
- Failing to follow administration directions exactly as specified in the Test Administrator Manual.
- Losing a student's Test Booklet.
- Losing a student's Testing Ticket.
- Displaying testing aids in the testing environment (e.g., a bulletin board containing relevant instructional materials) during testing.
- Failing to provide a student with a documented accommodation or providing a student with an accommodation that is not documented and therefore is not appropriate.

- Loss of internet connectivity for computer-based testing.
- Providing access to Seal Codes for computer-based testing ahead of time and before reading the appropriate direction in the script.

Technology Incident

- A technology incident is a technology-related event that may or may not compromise test results but could affect the student's performance on the test (for example, school loses internet access or electric power during the testing session).

8. Procedures for Safety Threats and Severe Weather

In the event that there is a building evacuation, lockdown, or school closure that occurs before the start of a test, follow the protocol outlined below:

- Proceed with testing only if the test can be completed that day.
 - If the test cannot be completed, schedule the test during make-up testing.
- Document the situation, noting the event, date, and time, students impacted, and any other specific details regarding the situation.

In the event that there is a building evacuation, lockdown, or school closure that occurs during the test, follow the protocol outlined below:

- If possible, note the time of the disruption so that the remaining time for the test can be calculated.
- If leaving the test environment, lock the door or take necessary steps to ensure the security of the test materials if time permits.
- Upon returning to the testing room, prepare students for the continuation of the test:
 - Test Administrators must inform students how many minutes remain in the test.
 - Test Administrators must write on the board the updated start time and stop time of the test.
 - Students may need to be resumed in the testing portal if testing online
- Document the situation, noting the event, date, and time, students affected, and any other specific details regarding the situation.
- Contact your BTC to complete a testing irregularity or security breach form.