Maryland's State Testing Program: Protecting Student Data

Maryland College and Career Ready Standards

Maryland State Department of Education — Preparing World Class Students

Our Policy

Students have taken tests for decades, and security breaches—answers leaked to the public, one way or another—are not new. In an era when so much information is readily available online, and easy to post, it is important to put appropriate safeguards in place.

Sharing images of PARCC or any test via Twitter, Instagram or other public social media sites is prohibited, in order to maintain test security. This is standard practice for large-scale tests, including the ACT and SAT.

Strong Privacy Protections are in Place

1. Our data security efforts fully comply with the Family Education Rights and Privacy Act (FERPA).

2. PARCC vendors are required to use the highest level of industry-standard encryption, firewalls, and intrusion detection to prevent and detect a broad range of potential security threats. These requirements are built into Maryland's contracts with test vendors.

3. Maryland requires student information and test data to be encrypted at all times, including during data storage and transfer.

Privacy Q&A

Does the PARCC test vendor monitor or follow students?

No. The test vendor searches all public posts, not individual students. Software helps uncover images or words from actual tests.

What happens when test data are discovered posted online?

It is usually possible to identify the state and school where the content originated through public social media pages. The local school authorities are then contacted; each school or district determines the best course of action for removing copyrighted material and taking any disciplinary action.

What information does PARCC collect from students?

Only information requested by Maryland and its local education agencies is collected—just as we've done in the past. The test vendor does NOT collect Social Security numbers, physical or online address, academic reports, or other personally identifiable information.

Family Education Rights & Privacy Act (FERPA)

NO ONE
is allowed to sell student education record data.

EMPLOYERS
can't be given student personally identifiable information unless applicants (or their parents) give consent.

3rd PARTIES
should not use personally identifiable information from educational records to market to kids and families.

ANOTHER SCHOOL
can receive data if the student intends to enroll in that school.

DATA RECIPIENTS
must safeguard data, including using data only for the purpose for which they were disclosed and destroying data when no longer needed for that purpose.

SCHOOL OFFICIALS & AUTHORIZED 3rd PARTIES
must have a legitimate educational interest for accessing student data before they can view them.

AUTHORIZED 3rd PARTIES
can use data only for the purpose for which it was shared, and only under the direction of the school district or state education agency.

STUDENT'S PARENTS
can access their child's data if the child is younger than 18 and not enrolled in postsecondary education.

STUDENT'S TEACHER
can access the student's data to meet educational needs.

SCHOLARSHIP & FINANCIAL AID PROVIDERS
can receive data when the student has applied for or received financial aid from that entity.

HEALTH & SAFETY
student data can be shared for reasons of health and safety in certain emergencies.