

Assurances Document for Embargoed Data

1. Purpose of Assurances

Periodically, the Tennessee Department of Education (TDOE) establishes data review periods whereby local education agencies (LEAs) are provided access to preliminary data files to enable them to review, analyze and verify the data before the data is deemed final and released publicly. As with any review period, some data may change due to this process. As a result, any preliminary data provided by the TDOE to LEAs during the review period shall be under a disclosure embargo for the length of the review period. We also strongly recommend that districts wait until the data is final before making any consequential decisions.

This data shall hereinafter be referred to as “Embargoed Data”. The purpose of these assurances is to establish a protocol to be followed by LEAs who access Embargoed Data during any data review period.

2. Duties of the TDOE

The TDOE shall establish all preliminary data review periods. At the beginning of every review period, the TDOE shall identify for the LEA:

- A) Which data is covered by the embargo;
- B) the term of the review period and embargo; and
- C) the specific process for the LEA to submit potential corrections to the department.

3. Duties of the LEA

LEAs shall observe the following security provisions when using, transferring, storing, and analyzing Embargoed Data. These provisions ensure that the disclosure embargo is always maintained during the preliminary data review period and there is no unauthorized public release of data that has not been checked for accuracy and finalized.

Storage and Transfer

3.1 Embargoed Data files **must** remain secure throughout the duration of the preliminary data review period.

3.2 Embargoed Data must be stored where **only** the Director of Schools and their named internal designee(s) (collectively referred to as “Authorized Individuals”) may access Embargoed Data.

3.3 If copies of Embargoed Data are made, the location of **all copies** of Embargoed Data must be carefully tracked. An Embargoed Data Access Log must be established by the LEA to track individuals who are

accessing Embargoed Data. The Data Access Log shall be monitored for activity in violation of these assurances.

3.4 Embargoed Data shall not be transferred via unsecure email or other means. All copied Embargoed Data files may be stored in a secured location with access limited to system administrators, director of schools, and Authorized Individuals.

Usage

3.5 Embargoed Data may be accessed **only** by Authorized Individuals.

3.6 Embargoed Data **may not** be shared with any other individuals outside Authorized Individuals.

3.7 Publically available discussions, presentations and reports based upon Embargoed Data **may not** occur during the review period where the data is under an active disclosure embargo.

3.8 All internal LEA discussions and reports should protect the privacy, anonymity and confidentiality of all Embargoed Data in compliance with the Family Rights and Privacy Act (FERPA) and the Tennessee Data Transparency and Accountability Act. The handling of all Embargoed Data will, at all times, adhere to FERPA and the Tennessee Data Transparency and Accountability Act.

4. Data Release Incidents

4.1 “Data Release Incident” means any release of data covered by the embargo, whether intentional or unintentional, beyond those parties who have been designated as Authorized Individuals.

4.2 Any Data Release Incident that comes to the attention of the LEA must be reported to the TDOE immediately but no later within twenty-four (24) hours of discovery.

4.3 The LEA shall adopt a procedure stating that any Authorized Individuals who are responsible for a Data Release Incident, whether through negligence or intent, may be subject to permanent loss of access to Embargoed Data during future review periods.