Secure Transmission of Student Data

Updated 2/8/21

Note: This document will be incorporated into a future version of the Test Administration Manual.

Section 2.5: Student Confidentiality of the Test Administration Manual states, "Secure Student Identification Numbers (SSIDs) and other confidential personally identifiable student data must remain secure at all times and must not be associated with a student's name in an unsecured place or manner."

A transmission is "secure" if there is no reasonable expectation that a third party (i.e. someone other than the sender and intended recipient) will have access to the information transmitted.

Secure communication methods. The methods below have sufficient security to transmit both an SSID and personally identifiable information (such as name or date of birth). These are listed in order of ODE security preference; however, districts are free to choose any method(s) from the list.

1. Direct, in-person transmission (written or verbal)
2. A password-protected website or secure district parent and student interface
    a. **Examples**: ParentVue or StudentVue
3. Sealed mail or package delivery
    a. **Examples**: US Postal Service or other direct delivery service
4. 1:1 voice or video communication
    a. **Examples**: telephone, single-person calls using voice/video applications (such as Google Voice, Google Meet, Zoom).
    b. **Note**: private chat in a group call is non-secure.
5. Secure file transfer owned by district/ESD
    a. **Note**: ODE's secure file transfer site is reserved for communications involving ODE.
6. Multi-step transmission: secure information is broken into "pieces" and transmitted through multiple communications
7. Encrypted or password-protected document sent via email
    a. **Example**: Word doc or pdf with password protection

Non-secure communication methods. Any method other than those listed above is not secure, and should not be used to transmit both an SSID and personally identifiable information.