Protecting Student Data

What are reasonable safeguards to protect student data?

- Use password protected computers and computer programs;
- Use only educational technology pre-approved by your school or district that is Education Law 2-d compliant;
- Dispose of student data when you are done by shredding paper files and deleting electronic files;
- Do not put any student data (including images) on social media.

What to consider when working with student data?

- **Do ask yourself:**
  - o   Am I sharing student information?
  - o   Can someone personally identify my student from this information?
  - o   Do I have parental consent?
- **Don't ever email** personal student or teacher data in an email; in fact, be VERY careful how personal email is used for school purposes;
- **Do ask** your teacher or district for guest access to any online systems or ask your teacher for assistance in accessing these systems. Password sharing is strongly discouraged. (Anticipate that your request may be denied);
- **Don't** use educational technology programs that your school does not have a contract for. (These will be published on the district / schools' website.) Check with your school administration if you are unaware whether a contract exists for a particular program.
- **Don't** send student grades and other educational information via email – if parents ask for their child's grades, call them.
- Access Fordham's Do's and Don'ts [Do's and Don'ts for Teachers](#)

Special considerations with collecting data for the edTPA and field – related assignments

- **Remember to protect students' name under all circumstances** (collecting IEP and other plan info for your Context for Learning, reflections, lesson plans, differentiation, etc.). CODE your students' names (A. B. C etc. and name of the school and the teacher) and keep that code list at home in a protected place.
- **Do not** EVER take home or transmit confidential, identifiable information about a student (e. g. a portion of an IEP, grades, behavioral report).
- **Protect ANY data you collect electronically (**on your phone or computer) with passwords and other reasonable safeguards.