In the age of the internet, tech tools and apps make it easier for teachers to engage their students and introduce new modes of collaboration and learning into their lesson plans. With the use of these ed. tech tools, student data is collected by both the educators and the companies providing the tech service. This means, as a teacher, you must take the necessary steps to ensure your students’ personal information is secure. Not only is it an educator’s prerogative to protect their students’ personal information, but it is critical that you teach your students the skills to protect themselves in the future.

Landon, a teacher from St. Louis, Missouri, tells us that:

*“With the proliferation of educational tools on the internet, especially in the past 5 years, I have really had to step my game up to learn how to protect my students’ data when using these tools. Students have a right to have their data protected and I make it my goal to ensure that every tool I use in my classroom follows specific data privacy standards.”*

Even with national laws, district guidelines and individual school specifications in place, it can be tricky for educators to navigate the complex landscape of the tech world and protect their students. Here, we’ve put together five simple steps teachers can take to safeguard their students and themselves.

1. **Be safe on social media** — Keeping a professional social media account can be a great way to keep parents and other educators in the loop about what you’re doing in your classroom. This will also mean that you’ll need to review the privacy settings of each social account, making it as secure and private as possible. For example, set your classroom Twitter account to ‘protected’ so that only people you follow can see your tweets. Or if you’re using Facebook, make sure you look at the privacy controls and make the account visible to friends only. Find out how, here. Finally, when sharing photos of your class, use a photo editing tool to blur your students’ faces or any other information that could reveal their identity. It’s simple with free online tools like Luna.

2**. Ensure that the ed. tech tools you’re using are encrypted** — When you go to an educational website, make sure that the data is stored and transmitted securely, i.e. make sure the url has an ‘s’ after the http or look for the secure link icon in the URL bar. With websites that contain ‘https:’, if any data were leaked or obtained by an unauthorized party, it would not be usable. That way you will know that any data entered in this website will be safe. Unfortunately, it is not so easy to tell if phone apps are encrypted. While Apple (iOS) enforces all apps to communicate through https, this is not necessarily guaranteed for Android apps.

3. **Check each tool’s privacy policy** — For each technology you use, ensure that there is a privacy policy in place. Read through each policy to see where they stand on student data privacy and only work with tools that comply with your school’s student data privacy guidelines.

Quick Tip: It’s time-consuming to review every privacy policy. Check to see if your school or district has a list of tools that have had their security and privacy guidelines reviewed and approved by specialists. For example, Go Pollock has signed the California Student Privacy Alliance agreement, which assures that the tool meets both federal and state laws regarding student data privacy. The agreement also contains Exhibit E, making it essentially an umbrella agreement for other California districts to rely on.

4. **Be transparent with students and parents** — When you’re upfront with your students and their parents, it makes it much easier in the long run to gain and keep their confidence in you. At the beginning of the semester, create a list of tools you’ll be using in class and make it available for parents to access. On this list, you should also link to each of the tool’s individual privacy policies for parents to review.

5. **Have a plan in place for mistakes** — Along with providing a list of tools you’ll be using in class, let the parents know how they’ll be informed if there is any misuse or breach of personal information. Will you be contacting them, or will they get a letter from a district administrator or the IT department? You should also provide a breakdown of remedies in case of such an event, such as the student being enrolled in an identity theft protection service.

Above are just a few simple steps you can take to ensure that you’re protecting your student’s personal information. What other measures do you take to protect your students’ data?