SECTION VI:
Best practices and practical tips to protect teacher and student privacy



Do your homework

- **BECOME FAMILIAR** with relevant federal and state employment and social media laws. You should also know your school, district, or other policies concerning your privacy.
- **INVESTIGATE** which personal information your school, district, and state are collecting about you and your students and how the data is being used. Arm yourself with this knowledge so you can make informed decisions about the data you share. To learn how teacher and student data are at risk, see Sections I and II.
- **CAREFULLY READ** the Privacy Policy or Terms of Service (TOS) of any app or program used in your classroom to determine whether it complies with state and federal privacy law. The U.S. Department of Education provides guidance to help educators evaluate common terms found in TOS, including examples of "red flags" to avoid. See the Resources section for a link to this guidance. You can also ask your administrators for a copy of the contract or service agreement with a vendor. The Massachusetts Student Privacy Alliance provides a model agreement you can compare it with. Find the link in the Resources section.

> Some ed tech vendors may claim rights to your and your students' intellectual property in their TOS. For example, the TOS of the free coding website Code.org grants the organization "a worldwide, non-exclusive, transferable, assignable, fully paid-up, royalty-free, perpetual, irrevocable right and license to host, transfer, display, perform, reproduce, modify, distribute and redistribute, adapt, prepare derivative works of, use, make, have made, import, and otherwise exploit" computer code or other materials that students post or upload to the program.



Resist the urge

Ed tech companies often exploit teachers and administrators by recruiting them to use and recommend their products in exchange for compensation, such as travel expenses to conferences or free devices. Acting as an "ambassador" in promoting a product and receiving any sort of compensation is ethically questionable and can run afoul of district policies or state laws. See Section III for more details.

- **IF YOU HAVE A CHOICE,** don't use social media for school-related purposes. If your school requires you to use a social network, discuss this with your union and the administration. If you choose to use it anyway, learn about how to protect your students' privacy, as well as your own. Section V explains how.
- **DO NOT USE** any apps or online programs that have not been vetted by your district technology officer, and whenever possible, ask for parental consent beforehand.

- **IF TEACHERS ARE AUTHORIZED** to adopt tools on their own, resist the urge to use "free" apps with "click-wrap" agreements that just require checking a box to accept the TOS. This action can make you party to a legally-binding contract whose terms may violate federal or state law. Moreover, you may unknowingly be paying with your students' data or your own.
- **IF YOUR STUDENTS** are under the age of 13, additional legal restrictions apply under COPPA — see Section III for more.
- **AT THE END** of the school year, make certain that you or school administrators contact each vendor to close any accounts and delete teacher and student data.
- **WHEN USING ED TECH,** ensure that the least personal information necessary for its operation is provided to the vendor. For example, if the use of an app isn't dependent upon uploading your photo or photos of your students, resist the urge to do so. If the app asks if a student has a disability or receives accommodations, don't offer this information unless mandated by your school or district.
- **IF YOU GIVE** surveys to your students, check to see if the questions touch on any sensitive areas as described in Section III under the Protection of Pupil Rights Amendment (PPRA). If they do, you must notify parents in advance and allow them an opportunity to consent or opt their child out of the survey.

Survey Results:

In response to our survey, an astonishing 44 percent of respondents said they did not know what happened to student and teacher data after the use of an app was discontinued; 37 percent reported no consistent policy was in place to address deletion of apps or data; and 12 percent said no one in their district acts to ensure teacher and student data are deleted when the app is discontinued. Only 7 percent of teachers said they or district administrators ask companies to delete teacher and student accounts after the app or program is no longer used.



Practice discretion

- **DON'T ATTEMPT** to access data for which you're not authorized, including students' attendance, grades, course schedules, and health information stored in digital information systems, such as Infinite Campus and PowerSchool. Federal law, including the Family Educational Rights and Privacy Act or FERPA, limits your access to only the information of those students for which you are directly responsible, and for purposes required to fulfill your professional responsibilities. See Section III for more detail.
- **WHEN ENTERING** your students' personal information into data systems, take extra precautions to ensure its accuracy. Student records can follow students for life and may be used for high-stakes decisions. To see how student data is at risk, see Section II.
- **BE CAREFUL** about accessing your students' previous grades or behavior information, which may lead you to lower your expectations or cause you to unconsciously prejudge them even before you've gotten to know them personally.
- **DATA WALLS** can do more harm to students than good. In addition to possible FERPA violations (see Section III), publicizing student rankings or performance can hurt student morale and undermine their motivation.

- **IF YOU ARE PROVIDED** with a device by your school, software may be preloaded that allows the district or school officials to monitor your movements or communications. The same is true of your school email account and/or your use of social media. Be mindful that you may be surveilled; be cautious when posting about your school, students, or administrators; and make sure that you use district devices and your official email account in a responsible manner.
- **IF YOUR SCHOOL** employs Google products, including Chromebooks and/or G Suite for Education with accounts for Gmail, Google Docs and other tools, the Electronic Frontier Foundation provides helpful guidance on how to set the defaults to minimize the data collected about you and your students. For links to their advice, see the Resources section.
- **CONSIDER** using a password manager or other secure method to store your login and passwords, and be certain to shred any scrap pieces of paper with this information that may be in view in your work area. And never share your passwords with anyone — including substitute teachers or student helpers. If you do so in an emergency, be sure to change them as soon as possible.
- **COVER YOUR LAPTOP** webcams with a sticky note or Band-Aid. After all, former FBI director James Comey and Facebook CEO Mark Zuckerberg do this.



Get involved

- **ENCOURAGE YOUR SCHOOL** or district to foster a privacy-conscious culture. Share this toolkit with your district office or, if applicable, your union leadership. Advocate for the creation of a school privacy oversight committee, including parents, teachers, students, and technical experts to give input on how to strengthen data privacy and security policies.
- **URGE YOUR DISTRICT**, school, and union to offer training and professional development on how to best protect student and teacher privacy.
- **IF YOU BELIEVE** your data privacy has been violated, or that of your students, raise your voice. Chances are you aren't the only one with concerns. Contact your local, state, and national unions for guidance, and see Section VII to learn how to advocate for stronger privacy protections.