Know what you need and why you need it.

Make sure you understand what data you need to use and why you need to use it. Don't access or use data for any other purposes.

Protect your neighbors' privacy.

Recognize that you may have access to information about students and teachers in your communities that is private or sensitive. Treat all information with care!

Share with care.

Before you provide any information, make sure that you are providing only what's required and that you are using the most appropriate option for sharing.

Information Sharing Options

Secure Cloud Solutions
Direct system access
Shared network folders
Secure FTP

Not Options

Removable/losable media
Email*
Insecure Cloud Solutions

Do as little as possible when sending data.

Data minimization is crucial for protecting privacy. If you must send information about individuals, use **only** the student ID numbers (not names) and the minimum amount of information necessary.

Trust, but verify.

Auto-complete is terrific—and also a terrific risk. Double- (and triple-) check to ensure that your email is going to the person you really want it to go to.

Act like your emails are public documents.

In fact, @k12 or other district emails may be subject to FOIA requests. Do all you can not to send PII about students, colleagues, or others via email. If you must, treat it as if you were sending your own information.

Documents subject to a FOIA request can be redacted to remove PII, but try to do all you can to save time and effort for legal and administrative staff who do the redaction!

FOIA is about your work, not about your devices.

Any state or district business conducted on personal devices is still subject to FOIA.

Keep it secret!
Keep it safe!

Do all you can to ensure that other people—coworkers, family members, complete strangers—cannot see or gain access to private or confidential information.

Just say, “No!”

Do not store passwords in your Internet browser or other applications. Storing your password is just like not having one to begin with!

Log out and lock it down.

Make sure to log out of all applications that may include private or confidential information. Close browser or explorer windows, just to be safe. Lock your other devices and filing cabinets when not in use.

Relax! Don’t do it!

Do not open or store sensitive information on personal devices. Doing so constitutes a security breach. (Besides, when you’re on your own time, you should be relaxing!)

Papers are data, too.

Data includes not only information stored in the student information system or other electronic sources. Profiles, reports, applications, and other paper-based records are also rightfully considered data and should be treated as such.

Watch your mouth.

"Loose lips sink ships." Make sure you use your best judgement and discretion when you must talk about sensitive information with colleagues. Try to avoid talking about sensitive topics or information in public settings.

Keep your eyes on the horizon…

Guarding students' privacy is a crucial part of education stakeholders' every day jobs. Always be on the look-out for possible threats—and ways to improve!