

Student Data Privacy & Digital Citizenship

Teacher Responsibilities

Teachers should NOT be creating student accounts or using student PII (Personally Identifiable Information) in apps, programs, platforms, websites, or extensions that are NOT district approved. Check to be sure it is district approved before you use it. If it is not, then you must submit a Program Approval Request through Incident IQ.

Scan here for more information about the Program Approval Process



Student Data Privacy guidelines for Teachers

MPS Student Data Privacy states: “As teachers, we are trained and committed to protect the students’ data we can access.” FERPA, COPPA, CIPA, and ISTE provide guidelines for teachers to (see back for more information): • Make sure the programs we use for teaching and learning are safe • Protect students’ data and PII (Personally Identifiable Information) • Create socially responsible experiences • Educate minors about appropriate online behavior Never use social media platforms or text messages to share experiences with your students or students’ families. Instead, send announcements, postings, and messages through ParentSquare. You can also invite your parents to be observers in Canvas to view their students’ classroom agendas, objectives, and assignments.	Personally Identifiable Information (PII) Includes: • First and last name; • A home or other physical address including street name and name of a city or town; • A screen, user name, or nickname that functions as online contact information; • A telephone number; • A Social Security number; • A persistent identifier that can be used to recognize a user over time and across different websites or online services; • A photograph, video, or audio file, where such file contains a child’s image or voice; • Geolocation information sufficient to identify street name and name of a city or town; or • Handwriting • Information concerning the child or the parents of said child that the operator collects online from the child and combines with an identifier described above.
---	--

Digital Citizenship guidelines for Teachers

We are teaching our future population of citizens. Not only should we teach and model great citizenship skills for students as they interact in their communities, but we should also be **TEACHING** and **MODELING** good **DIGITAL CITIZENSHIP** principles as well. Please discuss appropriate digital citizenship behaviors with your students and display those expectations in your classrooms.

- Use Common Sense Media’s digital citizenship curriculum or other digital citizenship lessons as well as parent resources to enhance, re-enforce, and improve upon student behaviors.
- Collaborate with your media specialist to see which lesson they will receive in the library each semester.

Below are a few basics to remind you of ways you can model good principles yourself:

- Do not share your password with your co-teachers or with students
- Do not leave your sticky note of password visible
- Cite your sources and give credit inside lessons
- Do not plagiarize
- Using programs/apps/websites that are safe and secure



ISTE- International Society for Technology in Education
 There are 7 ISTE standards for Educators, and standard 2.3-Citizen instructs educators **to inspire students to positively contribute to and responsibly participate in the digital world.**

Citizen – Create socially responsible experiences for learners, critically examine online resources, mentor and model safe, ethical, and legal practices, manage professional data, and protect student privacy.

- Examples include computer skills, communication skills, digital citizenship, copyright/plagiarism, privacy policies.



COPPA is the Children’s Online Privacy Protection Act enacted by Congress requiring operators of commercial websites and online services to be very clear about what they are doing with children’s personal information they are collecting.

Therefore, for each program/website/app we want to use with our students must first be vetted by our district to find out if they **collect our students’ data and how they are using and storing the data**, making sure each program our students use complies with COPPA rules and regulations.



CIPA – The Children’s Internet Protection Act was enacted by Congress to address concerns about children’s access to obscene or harmful content over the Internet.

It is the responsibility of educators to **protect student data and educate minors about appropriate online behavior, including interacting with individuals online, and cyberbullying awareness and response.**



FERPA – Family Educational Rights and Privacy Act is a federal law that protects the privacy of student education records.

It is a federal law that affords parents the right to have access to their children’s education records, the right to seek to have the records amended, and the right to have **some control over the disclosure of personally identifiable information from the education records.**

