Privacy Cheat Sheet

**PII Definition**

* Student’s name, or the name or nickname of a family member, their address, any personal identifiers that directly tie to one individual (SSN, photos, Phone #s, medical records, date of birth, detailed geographic information

**FERPA (Family Educational Rights and Privacy Act)**

* Parents have right to access their student’s records
	+ Have them amended
	+ Right to some control over disclosure of PII from records
	+ When student turns 18 or enters post-secondary institution, rights transfer to the student
* **Directory** - Directory information is information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed
	+ Schools may disclose, without consent, “directory” information such as address, telephone number, date and place of birth, honors and awards, and dates of attendance.
	+ Schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA.

**COPPA (Children’s Online Privacy Protection Act)**

* Designed to help parents remain control of what personal information websites and online services can collect from children under the age of 13
* Applies to operators of websites, apps or other online services that collect, use or disclose personal information from children under 13
* Applies to operators of general audience websites, apps, or online services that have knowledge that they are collecting, using or disclosing PII from children under 13

**CIPA (Children’s Internet Protection Act)**

* Schools and libraries are required to ensure that children do not have access to obscene or harmful content over the Internet –

**Maryland House Bill 298** Requiring specified operators of specified Internet sites, services, and applications to protect PreK-12 student information from unauthorized access, implement and maintain security procedures and practices, and delete student specified information under specified circumstances; prohibiting specified operators from knowingly engaging in specified activities with respect to specified sites, services, and applications related to targeted advertising, selling, and disclosing student information under specific circumstances; etc.