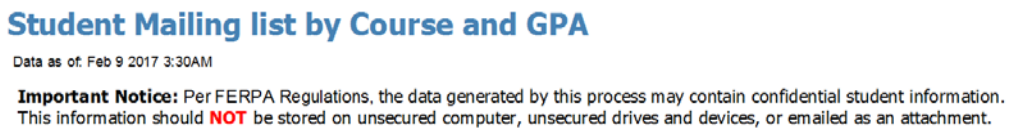
What is FERPA data and why is it important to protect here at ECC?

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html).

Here at ECC, we adhere to the guidelines set forth by the FERPA regulations (for example):



Just as HIPPA (Health Insurance Portability and Accountability Act of 1996) data has recently become the #1 attack vector for hackers due to the value of the information when sold on the black market (Dark Web), FERPA data is destined to become a "rock star" in the murky world of cyber targets in the not-so-distant future. Whereas HIPAA data only contains health information, FERPA data contains several different types of data, making it a treasure trove of valuable information:

- Personally Identifiable Information (PII)
  - Name, address, S.S.#, date of birth, etc.
- Education record
  - Grades, classes, etc.
- Health records
  - Including immunization information, records maintained by a school nurse
- Directory information
  - Name, address, phone, date/place of birth, honors/awards, attendance dates

This is why each and everyone of us as employees of ECC must do their due diligence in protecting the data of our students! Here are 10 steps that we can follow to safeguard the sensitive data of our students (Keith R. Krueger, Consortium for School Networking):

1) Designate a privacy official. Decide who in the district is responsible for privacy. A senior administrator should be designated as the person responsible for coordinating efforts to ensure compliance with privacy laws and policies.

2) Seek legal counsel. All schools have access to the services of legal counsel. Regardless of how your school receives those services, make sure your counsel understands the privacy laws and how they are applied to technology services.

3) Know the laws. This is not easy, but it is essential. In addition to the CoSN Toolkit and resources from the U.S. Department of Education, many other organizations have developed or

will be developing privacy-related materials. Don't forget about state laws or proposed state laws.

4) Adopt school community norms and policies. FERPA and COPPA are the bare minimum when it comes to protecting privacy. There must be consensus among your stakeholders regarding collecting, using and sharing student data. Without consensus, it's impossible to adopt enforceable policies.

5) Implement workable processes. If your school is going to be serious about privacy, there must be processes with checks and balances for accountability. No one wants to create roadblocks to innovation, but ensuring privacy requires proactive planning and disciplined action on the part of school staff. Compliance with privacy laws suggests some specific processes for schools, and they should be reviewed regularly to ensure that they are workable and reflect current interpretations.

6) Leverage procurement. Every school RFP, bid and contract (or service agreement) has standard language dealing with a wide range of legal issues such as indemnity, liability, payment and severability. By adopting standard language related to privacy and security, you will make your task much easier. Many online services are offered via click-wrap agreements that are "take it or leave it." It may be necessary to ask staff to look for alternative solutions if the privacy provisions do not align with your expectations.

7) Provide training. Unless you train your staff, they will not know what to do or why it is important. Annual privacy training should be required for any school employee who is handling student data, adopting online education apps or procuring and contracting with service providers. Privacy laws represent legal requirements that need to be taken seriously.

8) Inform parents. Parents should be involved in the development of privacy norms and should provide policy input. Just as schools provide significant information about online safety and appropriate use, they should put significant effort into making sure that parents understand the measures that educators are taking to protect student privacy.

9) Make security a priority. The importance of security to ensuring privacy cannot be overstated. Secure the device, the network and the data center. Toughen password policies. Have regular security audits conducted by a third-party expert. Make sure that RFPs, bids and contracts have clear and enforceable security provisions for your online service providers.

10) Review and adjust. Interpretations of privacy laws are changing, and new laws may be added. School policies and practices will need updating and adjustment so that they reflect legal requirements. Processes can become burdensome and when that happens, some people may want to skirt the process. Seek input from those involved to ensure that the processes are not hindering teaching and learning.

Paul T. Yoder
Information Systems Security Specialist
El Camino Community College District