VERMONT
AGENCY OF EDUCATION

1 National Life Drive, Davis 5, Montpelier, VT 05620-2501
(p) 802-828-1130 | (f) 802-828-6430 | education.vermont.gov

Continuity of Learning: Student Data Privacy and Safety Guidelines for Students and Families

Purpose

The purpose of this communication is to provide information and resources to students and parents on student privacy and safety in an online learning environment. This guidance aligns with our guidance on student data privacy and safety for schools and educators.

Introduction

As districts implement different learning models to best support students and families during the ongoing COVID-19 pandemic, parents and caregivers can continue to play an important role in student's learning while at home. Families are encouraged to familiarize themselves with the safety policies and procedures their SU/SD has in place to protect their student's privacy when learning in an online environment.

Most SU/SDs already have an Internet Safety Policy which addresses:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communication;
- Unauthorized access, including "hacking" and other unlawful activities by minors online;
- Unauthorized disclosure, use and dissemination of personal information concerning minors; and
- Measures restricting minors' access to materials harmful to them.

What is FERPA?

FERPA is a federal privacy law that applies to educational agencies, institutions and applicable programs funded by the U.S. Department of Education. It provides parents and eligible students the right:

- to access education records and seek amendment of education records;
- to provide consent to disclosure of personally identifiable information (PII) from student education records unless a FERPA exception applies; and
- to file a complaint under FERPA.

What is COPPA?

COPPA sets forth limited rules governing the online collection of personal information from children ages 13 and under. According to the US Federal Trade Commission, the primary goal

Contact Information:

If you have questions about this document or would like additional information please contact:

Sigrid Olsen, Student Pathways Division, at Sigrid.Olsen@vermont.gov

of COPPA is to place parents in control over what information is collected from their young children online. "The Rule was designed to protect children while accounting for the dynamic nature of the Internet. COPPA imposes certain requirements on operators of websites or online services directed at children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age" (Retrieved October 2020 from Complying with COPPA: Frequently Asked Questions 2020).

Among other stipulations, operators covered by COPPA must (see full list of requirements here):

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children.
- Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children.
- Provide parents access to their child's personal information to review and/or have the information deleted.

Personally Identifiable Information

Both FERPA and COPPA were enacted to protect a student's personally identifiable information (PII) and other direct identifiers from a vendor/operator of commercial websites and online services. These PII can include:

- A first and last name;
- A home or other physical address including street name and name of a city or town;
- Online contact information as defined in this section;
- A screen or username where it functions in the same manner as online contact information, as defined in this section;
- 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. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol ("IP") address, a processor or device serial number, or unique device identifier;
- 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
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition. ((C., C., & E. (2015). Data Privacy Guidebook: Privacy Guidelines and Practical Tips. Retrieved October 2020))

What is SOPIPA?

In 2020, the Vermont Legislature passed SOPIPA, Student's Online Personal Information Protection Act (S.110, the Student Privacy is in Sec. 4, p. 18) enacted as 9 VSA 2443. Vermont has joined several states across the country who have enacted SOPIPA legislation that originated in

California. Essentially, SOPIPA ensures that entities that provide education technology solutions to schools and educators use student data for education purposes only, and do not sell information or leverage their services or platforms to target advertising to students. Education technology companies must adhere to SOPIPA regarding student data whether there is or is not a contract in place with a school or district. Currently, federal SOPIPA legislation is being pursued. To learn more about what SOPIPA legislation looks like visit Common Sense Media.

Student Data and Privacy

As we rethink education in response to COVID-19, and though we continue to strive for in-person learning, SU/SDs must be prepared for all learning models they have identified in their Continuity of Learning and re-opening plans. Traditionally, student data consisted of things like attendance, grades, discipline records and health records. With the implementation of different forms of technology, both virtual and in-person, parents and students have raised concerns about what and why certain PII would be shared with operators/vendors.

Privacy is concerned with protecting the rights of individuals and ensuring they have control over their personal data that institutions may use. It involves defining and creating procedures and policies that best guide how data is collected, stored and used, as well as with whom it can be shared.

Security involves using technical and physical strategies to protect information from cyber-attacks and other types of data disasters. That includes preventing unauthorized access or accidental corruption of data and maintaining its integrity (Retrieved October 23, 2020 from To Better Protect Student Data, Know the Difference Between Security and Privacy).

Everyone has a role for ensuring privacy and security for students, including students and families. The following practices, when used together as a whole, can help to maximize safe student learning in online settings.

Student Privacy Considerations for Families

- Understand simple ways to protect children's data, what to look for in apps, communicating with your child's school about privacy and "red flags" you see in some applications. Model for your children responsible stewardship of your own data.
- Talk to your children about what privacy (both online and in person) means and its importance.
- Be sure the tools your child is using to complete assignments and communicate with teachers are approved by your school district.
- Consider monitoring your child's internet use.
- If multiple family members are using the same devices throughout the day, be sure to log out between different family members.
- If you do not want your child's image to be displayed during online learning sessions, your child can either turn off or cover their webcam or join using the provided phone number.
- Have students connect from a "common" area of your home and not a private space, such as a bedroom, when engaging in remote learning.

- Turn on the security features on any device your child may use for learning activities. These can be found in the device's general settings under the privacy menu. These features can:
    - Restrict access to offensive or inappropriate content.
    - Require approval for downloads.
    - Limit time spent on certain apps.
- Make sure that students are aware of what to do if they are a victim of an online threat. They can be encouraged to report threats to a teacher, a school counselor, another trusted adult and the online service provider, if appropriate.
- Make sure you and your child have all the information to find their learning resources. Keep track of log-in and password information and URLs for each platform they use. Consider using a password manager in your internet browser, or keep passwords written down in a safe place. Change passwords regularly.

Student Privacy Considerations for Students

- Remember that all online interaction is an extension of the physical classroom, and expectations of your behavior online are the same as what would be expected in the classroom.
- Understand and protect data that might enable someone to identify and take advantage of you, your location or other personal information.
- All video connections should take place in a "common" area of your home, such as the living or dining room.
- Position camera to keep other family members and other rooms of the house out of the frame, sit with a wall behind you when possible.
- Consider using just the audio capabilities of a webcam.
- Do not give out personal information online without an adult's consent.
- Practice good online citizenship.
- Follow your school's 1:1 device agreement, if applicable.

Most SU/SDs already have policies and/or procedures around these practices that are communicated to parents, students, and any other school personnel

Resources

To Better Protect Student Data, Know the Difference Between Security and Privacy

Complying with COPPA F.A.Q

LearningKeepsGoing

A Learning System for Privacy, Security and Digital Citizenship Infrastructure

Parents' Guide to the Family Educational Rights and Privacy

ConnectSafely

Data Privacy Guidebook: Privacy Guidelines and Practical Tips

NetSmartz for Parents, Educators and Communities

Stop.Think.Connect.Campaign

Stopbullying.gov