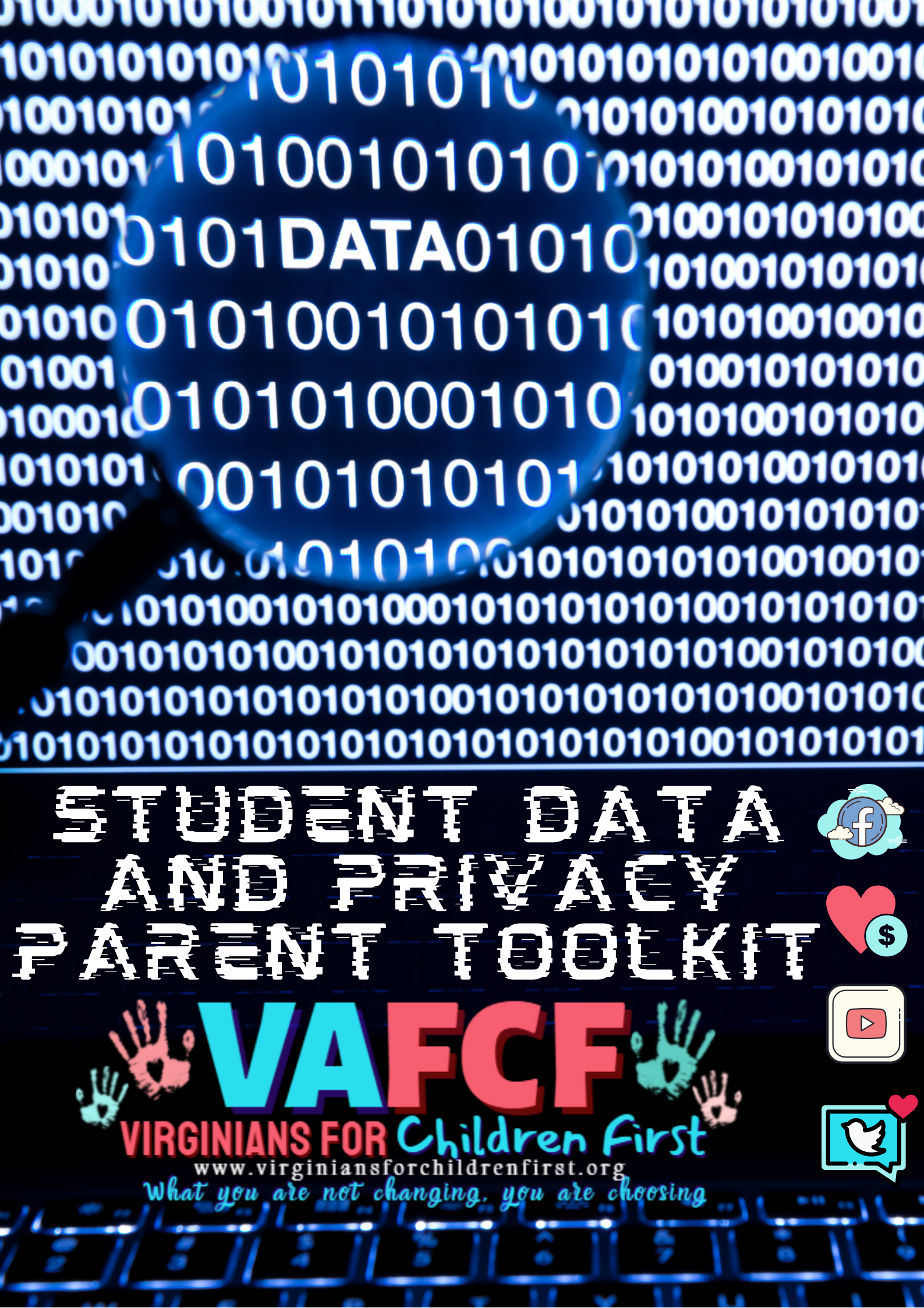

STUDENT DATA
AND PRIVACY
PARENT TOOLKIT
VAFCF
VIRGINIANS FOR Children First
www.virginiansforchildrenfirst.org
What you are not changing, you are choosing

STUDENT DATA PRIVACY PARENT TOOLKIT

VIRGINIANS FOR CHILDREN FIRST

WE HOPE THIS PRIMER AND TOOLKIT HELPS EXPLAIN THE CONCEPTS OF STUDENT DATA, INCLUDING WHO USES THE DATA, STUDENT DATA PRIVACY RISKS AND HARMS AND YOU THEN USE ALL OF THE RESOURCES TO PROTECT YOUR CHILDREN FROM SO MUCH UNKNOWN

Every day our children go to school and have data collected on them and computed in ways we could have never imagined- because we have trusted the public school system for so long that even though our parental gut instincts told us, months, years or even decades ago that there was something very anti-American about the slow creep of Federalized education we saw glimpses of, if not the full scope of it.

Now, with no textbooks to read through, paper tests to look over once graded, folder of homework sent home or even carbon interim report cards to sign and send back- those little rectangle electronic devices we once thought miraculous are tallying up positive or negative data stored in whatever mysterious realm where all we are told is that "it is safe because it is in the United States".

The latest data breaches of student and teacher data-

- Student uncovers ‘severe data security issue’ within DeKalb County schools-The files at risk contained information for about 93,000 students and 15,500 employees.
- A massive data breach has exposed four years’ worth of records of nearly 500,000 Chicago Public Schools students and just under 60,000 employees
- 24 school districts and 18 charter schools in New York — totaling “at least” a million students in the state — were impacted by the breach of private student data that occurred during a January cyberattack on Illuminate Education’s systems- breaches also occurred through Illuminate in Connecticut, California, Oklahoma, Colorado
- Data Security:Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm;
- **HOW DOES THIS MAKE YOU FEEL?**
  - Dec 16, 2021 The Virginia Department of Behavioral Health and Developmental Services (DBHDS) victim of a global ransomware attack
  - THE SAME DAY Chesterfield County public schools reported website and internet outage "Shawn Smith with CCPS said the outage is due to a fiber optic line that was cut in the Richmond area"
  - I won't explain the HUGE LEGAL PROBLEM THERE.
- **DO NOT LET THE TERM DATA BREACH FOOL YOU- THESE ARE TARGETED CYBER ATTACKS ON OUR CHILDREN AND THE FEDERAL GOVERNMENT DOES NOTHING.**

With the rise of the Social Emotional Learning nightmare, or actually our awakening to its existence, most of of us have been asking ourselves, "why the need to assess social and emotional skills in children?" Some people will tell you that this is needed to help the “students at risk.” Some will tell you it is needed because of all the trauma children experienced from being locked in their homes during "COVID". But if you stop and listen to what you are being told in the midst of the propaganda driving us to hate each other because of our skin color, or what gender we may or may not be, or what you society has told you you MUST feel about someone who thinks differently than you or you too will become an outlier- you will hear language specific to turning our children into mechanisms driven toward Artificial Intelligence NOT Social or Emotional Intelligence.

STUDENT PRIVACY - WHY SHOULD PARENTS BE CONCERNED?

It's difficult for parents to imagine just how much information is collected about students in schools today, or how that information is used, stored, and shared with others.

During the course of a normal school day — and throughout a child's life from kindergarten to graduation from high school — an incredibly large amount of data, including highly sensitive information, is shared without parental knowledge or consent with vendors providing operational services or companies offering educational programs. Rather than secured in a file cabinet or kept on the school's computer servers, personal student information is often transmitted to and *stored in the "cloud" to facilitate access and use by third parties*- this includes the lunch line- to monitor under the guise of "free lunch program" as well as bus badges and computer devise as "textbook" your locality uses- they all come with RF (radio frequency) tracking chips so they know where your child is (along with the computer) at all times- which includes where you live.

Federal laws intended to protect students' data held by or for schools are simply inadequate to address the challenges of today's digital age- and have been gutted in the last decade with a direct purpose. In 2008 and 2011 Obama systematically FERPA -Family Educational Rights and Privacy Act- These amendments increased private company and third-party access to student data.

The 2008 changes expanded the definition of "school officials" to include "contractors, consultants, third party venders etc. In 2011 new regulations broadly define "education programs" to encompass programs not only focused on "improving academic outcomes" but also related to "bullying prevention, cyber-security education, and substance abuse and violence prevention" regardless of whether the program is administered by an educational agency or institution.

Data privacy as a fundamental right. Individual privacy rights are recognized in the US Constitution, the UN Declaration of Human Rights, and in over 80 countries around the world. Privacy rights also provide the foundation for other important rights, including self-determination and free expression.

Data privacy includes a person's control over how their personal information "flows" between them and any third parties (how it is used and shared).

Data privacy is subjective, as each person has unique privacy preferences and expectations. What feels invasive or creepy to one person may be innovative or cool to another. Many factors influence these preferences and expectations, including a person's familiarity with the entity or person collecting their data, whether a person is from a marginalized community whose data has been used in inequitable ways, their cultural background, and their trust in data-holding organizations.

Data privacy is contextual. Whether it is appropriate to use or share personal data in a particular manner depends on ever-evolving social and ethical norms and on legal frameworks. To ensure that people understand an education agency's or institution's community norms about data use, the agency or institution must communicate and engage directly with their community members.

STUDENT PRIVACY - WHY SHOULD PARENTS BE CONCERNED?

- **Social Harm**: Revealing personal and sensitive student information can result in stigmatization and cyberbullying.
- **Over-Surveillance**: Over-collection and monitoring of student data and online activity can have chilling effects, such as discouraging students' interest in learning or taking healthy risks.
- **A Permanent Record**: This regards how long institutions retain records of events, specifically mistakes, potentially tethering students to their past in limiting or harmful ways.
- **Loss of Opportunity**: Student data can be used to make decisions about students that can result in denials of opportunity.
- **Age-Inappropriate Content**: Students may access inappropriate websites and online content.
- **Safety**: Personal or otherwise sensitive information may be revealed that could endanger students' safety.

They are collecting data on **EVERYTHING** our children do- here are couple handfuls of examples none having real educational value they claim-

- Grades, test scores, attendance, discipline and health records, and college and career goals that schools track to help them follow a student's progression throughout their education career;
- Recorded observational data, which educators generate throughout the school day, about a student's behavior, motivation, or interests;
- continuous questioning on all children's home life, well being, food and transportation access, amounts to a disturbing trend of asking children what seem like benign questions, that when mixed with the new involvement of social workers in schools leaves a lot to be answered

The U.S. Department of Education (USED) has been pushing, bribing, and otherwise "incentivizing" states to expand their student data systems to track students from preschool through the workforce. Using this data, USED claims, can transform education to ensure that each child develops into the type of worker and global citizen the government wants him to be.

The House Committee on Oversight and Government Reform held on November 17, Inspector General Kathleen Tighe testified that USED's so-called "data security" system is riddled with vulnerabilities. The problems encompass both lax controls over the people allowed access to sensitive data, as well as outdated technology and inadequate security to prevent unauthorized access.

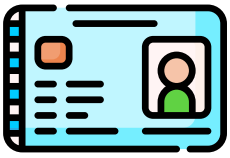
The Office of the Inspector General (OIG) found that of the 97,000 account/users with access to this information (government employees and contractors), fewer than 20 percent have undergone a background check to receive a security clearance. Parents should be horrified at this casual approach to allowing data access.

OIG and the General Accounting Office (GAO) found that the security mechanisms protecting that data are abysmal. Tighe's indictment was devastating: "During our testing of the EDUCATE environment, OIG testers were able to gain full access to the Department's network and our access went undetected by Dell [the vendor] and the Department's Office of the Chief Information Officer."

We are humans with beautiful, unique minds that are allowing the 1% to drive "future ready learning with 21st century soft skills to become better global citizens" while in the same breath they will then speak of global population control. They are determining who will be the alphas and who will be the gammas with "early childhood education" and their station in life WILL ACTUALLY be set at birth based on DATA.

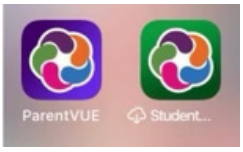
WHAT IS STUDENT DATA?

By the time a child enters Kindergarten they have already amassed a ton of data that once in the public school system then goes into the data cloud vaccines, medications, preschool evaluations, gender, race, and if you have been in Head Start or a Government free preschool program, your "data locker" is already full of "early childhood" assessments- will these early assessments lock our toddlers into the worthy or unworthy, Alphas or Gammas, based on resiliency judged by a teacher at age four?



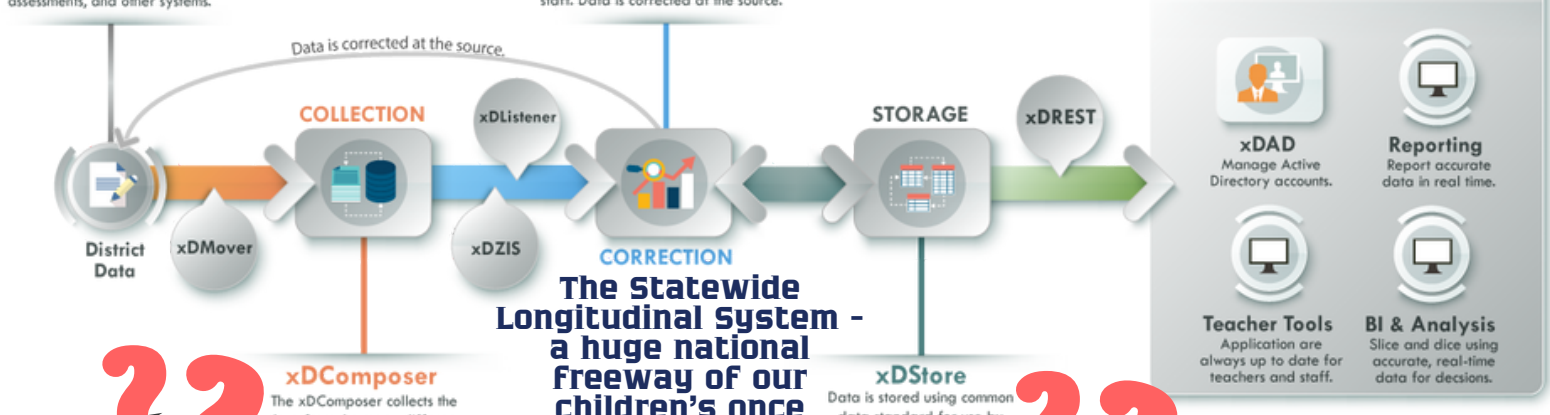
When a child receives their Student ID it becomes their own mini Social Security number for the next 12 years and "free lunch" has started a folder on parental data collection based on finances

By first grade most children will have their Chromebook or Ipad (1:1 device) packed full of educational apps and online "textbooks" ready to track every click, click rate etc. plus RF chips to track their every move and "safety features" to follow everything they do on their device



Here are a few apps you may have seen that collect millions of points of data on our children- and you if you have the Zuckerberg ParentVue on your phone

Non-Cognitive mental health assessments are done on our children by teachers K-8 and they self report on themselves 9-12, have you ever received notice to opt out?



The Statewide Longitudinal System - a huge national freeway of our children's once private information accepted by the state for more Fed Ed Grant money

How will this locker full of emotional quotient determine our children's futures?
THAT is the big question.

VAFCF
VIRGINIANS FOR Children First

EDTECH IS OUT OF CONTROL- YOUNG EDTECH COMPANIES,WITH PRESUMABLY GOOD INTENTIONS, ARE BEING TARGETED AND SWALLOWED UP, BECOMING WEAPONS FASHIONED, BY ELITIST PHILANTHROPISTS, AS WEAPONS AGAINST OUR CHILDREN.

How many of these are your child's school issued device? Do you know? Because they are supposed to notify you and give you the chance to opt out. ONE county in the state of VA gave appropriate TRANSPARENT individual letters sent to parents with an opt out option- ONE- FAIRFAX!

STUDENT PRIVACY RIGHTS UNDER FEDERAL LAW

FERPA (Family Education Rights and Privacy Act)

Passed in 1974, the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is administered by the U.S. Department of Education and applies to federally-funded schools and universities. It bars the disclosure of personally identifiable information (PII) in student education records—like grades, test scores, disciplinary records, contact and family information, and class schedules—to third parties without parental consent, but with some loopholes described below.

When FERPA was enacted almost forty years ago, Congress made it clear that students' personal information should not be made widely available. Congress was particularly concerned that if student records fell into the hands of private parties, these records could hurt students later in life when, for example, students were seeking jobs.

The law has been considerably weakened through regulatory changes in the past ten years, and was written before the emergence of computerized data systems and data-collecting learning softwar- both of these factors allow student PII to be easily shared with others outside of the school.

FERPA contains multiple “exceptions,” or certain circumstances under which student PII may be disclosed to parties outside of the school or district without parental consent. The most widely used is the “school official” exception, which allows student PII to be shared with vendors, consultants, contractors, and volunteers with “legitimate educational interests” who are performing “institutional services or functions” for the school. Common examples include online instruction and assessment providers, bus or cafeteria service companies, vendors that provide student information systems, and parents or other classroom volunteers.

The Education Department and Privacy Safeguards DESTROYED BY OBAMA

In 2008 and 2011, the U.S. Education Department amended the regulations for the Family Educational Rights and Privacy Act (FERPA). These amendments increased private company and third-party access to student data. This e 2008 changes expanded the definition of "school officials" to include "contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform

Surprisingly, in 2011, the Education Department again loosened the safeguards for student records by modifying the key terms "education programs" and "authorized representatives" to permit greater disclosure of student data. Under FERPA, "authorized representatives" of the U.S. comptroller general, the secretary of education, and state educational authorities may access student records to audit or evaluate federally supported "education programs."9 The new regulations broadly define "education programs" to encompass programs not only focused on "improving academic outcomes" but also related to "bullying prevention, cyber-security education, and substance abuse and violence prevention" regardless of whether the program is administered by an educational agency or institution.10And previously, "authorized representatives" were exclusively entities over which educational authorities had "direct control, such as an employee or a contractor of the authority."11 Now, authorized representatives can be any individual or entity that educational authorities select as an authorized representative.

FERPA
FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

Parents or eligible students have the right to take the following actions:

- Inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless it is impossible for parents or eligible students to review the original records (e.g., they live far away).
- Request that a school correct records they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Halt the release of personally identifiable information.
- Obtain a copy of the institution's policy concerning access to educational records.

While schools must obtain prior written consent from a parent before releasing most PII, directory information may be released without consent under certain conditions.

Consent to Disclosure of Personally Identifiable Information
Parents alone have the authority to permit the release of their child's personally identifiable information. The school may not release the PII information to a third party without the authorization from the parent. Personally identifiable information—often abbreviated as PII—refers to any data or information about students collected by schools, districts, government agencies, or organizations and companies working with schools that might reveal the identity or personal information of specific students or that could allow someone to indirectly track down the identity or personal information of students.
(a) The student's name;
(b) The name of the student's parent or other family members;
(c) The address of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.

Integrated Data Systems and Student Privacy

STUDENT PRIVACY RIGHTS UNDER FEDERAL LAW

Congress enacted the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. 6501-6505) in 1998. It is enforced by the Federal Trade Commission (FTC). The primary goal of COPPA is to allow parents to control what personal information is collected online from their children under age 13. The law applies to any vendors or operators of child-directed websites, online services including web-based testing, and programs or applications ("apps") that collect, use, or disclose children's personal information, whether at home or at school. Personal information can include a child's name, email, phone number, screen name, geolocation, photo, voice recording, or other persistent unique identifier.

Key Terms:

Personal Information means individually identifiable information about an individual collected online, including

● First and last name
● Home or other physical address including street name and name of a city or town
● Online contact information (Screen name or user name that functions in the same manner as online contact information)
● Telephone number
● Social Security Number
● Persistent identifier that can be used over time and across different Web sites or online services. These include, but are not limited to,
o Customer number held in a cookie o Internet Protocol (IP) address
o Processor or device serial number o Unique device identifier
● Photo, video, or audio file where such file contains the child's image or voice
● Geolocation information sufficient to identify street name and city or town
● Information concerning the child or the parents that the operator collects online from the child and combines
with an identifier described above
Data Collection:
● Active Data Collection – operator directly solicits information from children or enables children to make their
personal information available
● Passive Data Collection – tracking or use of "any identifying code linked to an individual, such as a cookie," as
well as any other "identifiers" that can be used to identify, contact, or locate a child over time and across different websites or online services

COPPA requires operators (online service providers, website operators, etc.) to

● Provide notice to parents

o Wishes to collect personal information from an individual child o Type of information it wishes to collect

o Purpose of information collection

o Means by which parents can provide and revoke consent

● Obtain verifiable parental consent before they begin collecting, using or disclosing information from children under age 13

o COPPA permits a school to obtain parental consent on the operator's behalf, as long as the operator uses the information only on behalf of the school pursuant to the agreement between the school and the operator. [from COPPA FAQs M(1) – M(3)]

An operator must obtain consent directly from the parents if it wants to use the data collected from the school for its own commercial purposes [from COPPA FAQs)]

● Manage Disclosures to ThirdParties

● Maintain a Privacy Policy in easy to understand terms on their website

o Names of all operators that collect or maintain personal information from children

o Define the type of information the provider collects, and whether collection is active or passive (see Data Collection above)

o Uses, or potential uses, of the information

o Disclosure and uses by thirdparties

o Parents may give limited consent to the collection and use of their child's personal information without consenting to its disclosure

o Operator cannot condition a child's participation in an activity on his disclosure of more information than is "reasonably necessary"

o Parent may review his or her child's personal information, request its deletion, and refuse consent to further data collection

● Retention and Disposal of personal information

o Retain personal information "for only as long as is reasonably necessary" o Protect against unauthorized access even when disposing of information

COPPA and Schools – See Complying with COPPA: Frequently Asked Questions, section M: COPPA and Schools for specific guidance from the FTC (the document linked below provides guidance for schools on COPPA compliance issues related to providing access to online services for students under age 13)

https://www.ftc.gov/tipsadvice/businesscenter/guidance/complyingcoppafrequentlyasked-questions#Schools

FTC TO CRACK DOWN ON COMPANIES THAT ILLEGALLY SURVEIL CHILDREN LEARNING ONLINE

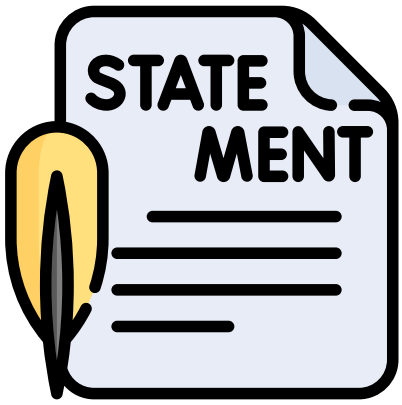
The Federal Trade Commission announced today that it will crack down on education technology companies if they illegally surveil children when they go online to learn. In a new policy statement adopted today, the Commission made it clear that it is against the law for companies to force parents and schools to surrender their children's privacy rights in order to do schoolwork online or attend class remotelyThe policy statement underscores that, even as companies across the economy become more aggressive in harvesting and monetizing individuals' data, ed tech providers cannot do the same: Ed tech providers must comply fully with all provisions of the COPPA Rule. Today's policy statement makes clear that the Commission will vigilantly enforce the law to ensure that companies covered under COPPA are complying with all of the rule's provisions, including:

- Prohibitions Against Mandatory Collection: Companies cannot require children to provide more information than is reasonably needed for participation in an activity.
- Use Prohibitions: Ed tech providers that collect personal information from a child with the school's authorization are prohibited from using the information for any other commercial purpose including marketing or advertising.
- Retention Limitations: Ed tech providers are prohibited from retaining children's personal information for longer than is necessary to fulfill the purpose for which it was collected and therefore cannot keep such data just because they might want to use it in the future.
- Security Requirements: Ed tech providers must have procedures to maintain the confidentiality, security, and integrity of children's personal information.

The Commission voted 5-0 at an open meeting to adopt the policy statement. Chair Lina M. Khan as well as Commissioners Rebecca Kelly Slaughter, Christine Wilson and Alvaro Bedoyaissued statements on the matter.

The Federal Trade Commission works to promote competition and protect and educate consumers. Learn more about consumer topics at consumer.ftc.gov, or report fraud, scams, and bad business practices at ReportFraud.ftc.gov

THEY HAVE MADE THE FIRST MOVE- NOW WE MAKE THEM FOLLOW THROUGH CALL AND EXPRESS YOUR CONCERN!



SAMPLE LETTER TO OPT OUT OF DISCLOSURE OF DIRECTORY INFORMATION (DATA MINING)

I understand that the Family Educational Rights and Privacy Act (FERPA), a federal law, allows my school or school district to disclose designated "directory information" to third parties without my written consent, unless I inform the school/district otherwise, and according to any existing policies and/or procedures.

I am submitting this form because: [choose one option]
My child's school or school district does not have a "directory information" policy.
My child's school or school district's existing "directory information" policy does not sufficiently protect my child's privacy.

PARENT OR GUARDIAN NAME: _____
STUDENT NAME: _____
STUDENT GRADE: _____
STUDENT ID NUMBER: _____
SCHOOL NAME: :_____
DATE: _____
PARENT/GUARDIAN SIGNATURE (IF STUDENT IS UNDER 18): _____
PARENT OR GUARDIAN EMAIL ADDRESS: _____
STUDENT SIGNATURE (IF STUDENT IS OVER 18): _____
Directory information that I ALLOW the school or district share:
(Note: Check only the information you ALLOW your school or district to share.)

- ☐ Student name
- ☐ Telephone numbers (e.g., home, cell, etc.)
- ☐ Parent personal information (e.g., name, address, phone, email address, etc.)
- ☐ Photograph
- ☐ Video or electronic images
- ☐ Date of birth
- ☐ Place of birth
- ☐ Home or permanent address
- ☐ E-mail address
- ☐ Dates of attendance
- ☐ Weight/Height Enrollment
- ☐ Status Grade
- ☐ Most recent school or educational institution attended
- ☐ Participation in officially recognized activities and sports Degree(s) received
- ☐ Awards and honors received Clubs/Affiliations
- ☐ School or district issued student ID number*

*NOTE: A student ID number may or may not be considered as directory information depending on how the school/district uses it.

SAMPLE LETTER CONTINUED

I ALLOW those elements of my child's directory information checked above to be shared **only with** the following parties:

In school or district publications, including a yearbook, graduation program, theater playbill, athletic team or band roster, newsletter, and other such publications.

- ☐ With the U.S. Military.
- ☐ With colleges and other educational institutions.
- ☐ With prospective employers.
- ☐ With political officers.
- ☐ With the National Student Clearinghouse.
- ☐ With news media.
- ☐ With the school PTA or district parent organization.
- ☐ With other groups and entities outside of the school or district, including community, advocacy and/or parent organizations. With companies that are selling products or services.
- ☐ With charter schools or mailing houses used by charter schools to send recruiting materials to families.
- ☐ On official school-related websites or social media accounts.
- ☐ On school employees' personal websites or social media accounts.
- ☐ To sign up my child for online educational tools or classroom applications (apps).*

***NOTE: FERPA allows a school or school district to share a wider array of students' personal information – beyond directory information – with individuals or companies offering operational services, online educational tools or classroom applications (apps) without parental knowledge or consent, or allowing for opt out, as well as for research or evaluation purposes.2**

REFERENCES

1. U. S. Department of Education, Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information. See http://familypolicy.ed.gov/content/ferpa-model-notice-directory-information

2. U.S. Department of Education, Privacy Technical Assistance Center, FERPA Exceptions - Summary. See http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf

COPPA- REQUEST TO INSPECT EDUCATION RECORDS HELD BY THE SCHOOL, DISTRICT, OR STATE (DATA COLLECTED)

I understand the **Federal Education Rights and Privacy Act (FERPA),** a federal law, gives parents the right to inspect the information in their child's education records, as collected and maintained by the state, district or school. According to the U.S. Department of Education, education records *"include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail."* Source: 34 CFR § 99.3 "Education Records" and "Record"

I further understand that the school or district may not charge a fee to search for or to retrieve education records but they may apply a reasonable fee to provide copies of education records, and must provide them in a readable form **within 45 days of the request.**

As such, please accept this ***request for access to all personally identifiable information*** in my child's education records, including the records you are required to maintain regarding disclosures of or requests for my child's personal information from organizations conducting studies for or on behalf of the school, ***and from Federal, State, or local educational authorities***. The records must also include all unauthorized disclosures of my child's information, including instances of data breaches or security hacks. Source: 34 CFR § 99.32 Recordkeeping Requirements.

If you estimate that the fees for copies of these records will exceed [$ _____], please inform me first.

PARENT OR GUARDIAN NAME:
_____

STUDENT NAME:
_____

STUDENT GRADE:
_____

STUDENT ID NUMBER:
_____

SCHOOL NAME:
_____

DATE:
_____

PARENT/GUARDIAN SIGNATURE (IF STUDENT IS UNDER 18):
_____

PARENT OR GUARDIAN EMAIL ADDRESS:
_____

PARENT'S HOME ADDRESS
_____
_____

PARENT OR GUARDIAN PHONE:
_____

STUDENT SIGNATURE (IF STUDENT IS OVER 18):
_____

COPPA FORM REQUESTING THAT SCHOOLS/DISTRICTS EXERCISE THEIR RIGHTS ON BEHALF OF PARENTS

Background information: The Children's Online Privacy Protection Act, or COPPA, is a federal law that allows parents to control what information is collected online from their children under the age of 13.

Congress enacted the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. 6501-6505) in 1998. It is enforced by the Federal Trade Commission (FTC).
The primary goal of COPPA is to allow parents to control what personal information is collected online from their children under age 13. The law applies to any vendors or operators of child-directed websites, online services including web-based testing, and programs or applications ("apps") that collect, use, or disclose children's personal information, whether at home or at school. Personal information can include a child's name, email, phone number, screen name, geolocation, photo, voice recording, or other persistent unique identifier. ***But it's important to note that COPPA only applies to personal information collected online directly from children; it does not cover information collected by adults that pertains to children.***

The **Federal Trade Commission'**s provides official guidance on how COPPA applies to the educational or "Schools" context, including the following:

"Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, ***individualized education modules, online research and organizational tools, or web-based testing services***. In these cases, the s***chools may act as the parent's agent and can consent to the collection of kids' information on the parent's behalf.*** However, the school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose…
In order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA. In addition, *the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information.*" (see more here: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools).

Since COPPA gives schools the authority to demand the types of personal information collected on your child under 13, review your under 13 child's personal information or have it deleted, and prevent further use or collection of his/her personal information, please use this form to request that your school exercises its rights on your behalf:

[Date]
[To your school's principal and/or your under-13 child's teacher]:
Per the Federal Trade Commission's website, "Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998 … The primary goal of COPPA is to place parents in control over what information is collected from their young children online… The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13."
The FTC's guidance further states that a school may sign up a child for online websites subject to COPPA but that a "school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose." It further states that in "order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA. In addition, the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information." https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools.)

It has come to my attention that my under-13 child is participating in one or more online programs at school which is/are collecting [his or her] personal information. While I understand that my under-13 child's teacher, school and/or district has authority under the Children's Online Privacy Protection Act to create an online account on [his or her] behalf with an online operator, or instruct my under-13 child to create his or her own account, it is also my understanding that the online operator must provide my school, upon request:
1. A description of the types of personal information collected on my under -13 child;
2. The opportunity to review my under-13 child's personal information and have the information deleted;
3. The right to opt out of any further use or collection of my under-13 child's personal information by the online operator.
Since my under-13 child or *one of the school's employees created an online account for my child at school, I request that the school and/or district immediately notify each online operator listed below to [choose one or more: 1. provide my school a description of the types of personal information collected on my under-13 child; 2. allow my school to review and/or delete all the personal information collected on my under-13 child; and/or 3. allow my school to refuse the online operator from further using or collecting my under-13 child's personal information] in the following online program(s):*

_____
_____
_____

Thank you for your assistance,
Name_____ relation to child_____,
child's name_____ and grade_____
Your Address_____, Phone_____,
Email_____

Prior/Opt-Out Notice

Health Care, Mental Health Care, Psychological Screening, and Counseling for My Child/Children

To: Superintendent of Schools
of_____
Principal,_____(name of school)
From: The Parents
of_____
This letter serves to provide notice that absent (without) our/my written consent, our/my child may not be subject to any form of health care, mental health care, psychological, social services or counseling screening or tests, including those provided by a School Based Health Center.
We/I formally exempt our/my child from all health care, mental or social programs and screening, whether directly by the school, School Based Health Center (SBHC), Wellness Center, Health Resource Room or through an affiliated resource. Concerns by school staff relating to our/my child's purported health/mental health, are to be brought to me/us for me/our attention and assessment. School staff or School Based Health Center staff are not to take it upon themselves to obtain a diagnosis or to provide health/mental health treatment, analysis, referral or labeling of any nature. Assessment and testing are to center on academics and physical fitness only. The informed consent requirement encompasses, but is not necessarily limited to, the following activities:

1. School or School-Based Health Care counseling related to mental or physical health
2.Behavioral, mental health, depression/suicide or psychological/behavioral screenings of any nature and/or diagnostic instruments (ie., TeenScreen, Healthy Teen Survey, School Climate Survey, emotional factors such as anger or peer relationships, sexual activity or orientation).
3. Anger management, "self-esteem"; "conflict resolution" courses; group or family counseling.

This is not a complaint against the school. Rather, it is an exercise of parental rights made necessary by events globally in which children have been harmed and their rights, safety and health injured by health/mental health assessments, diagnosis and treatments which are based upon subjective tests having no basis in science.

I thank you in advance for your cooperation in this matter. For our mutual protection and to assure there is no misunderstanding, a copy of this letter is on file with my/our attorney. This notice applies until and unless revoked in writing by us/me, and it is to follow our/my child through progressive levels of school in this jurisdiction, district or county.

Dated _____
_____,Parent(s) or Guardian of _____
cc: _____School District Board of Education

QUESTIONS TO ASK ABOUT STUDENT INFORMATION THE SCHOOL OR DISTRICT COLLECTS, USES AND SHARE

WHAT KIND OF INFORMATION DOES THE SCHOOL OR DISTRICT COLLECT about students and why? Who is it shared with? Will parents be notified about which personal data is collected or shared, as is considered best practice?

HELPFUL HINT:
The U.S. Department of Education Privacy Technical Assistance Center recommends that schools and/or districts should: • Develop and publish a data inventory listing the specific information it collects from or about students; and
• Explain why it collects each piece of student information (e.g., for state or federal reporting, to provide educational
services, to improve instruction, to administer cafeteria services, etc.).

IF DATA IS STORED IN A STUDENT INFORMATION SYSTEM (SIS), like InfiniteCampus or PowerSchool, who has access to my child's data, and what are they permitted to do with it? Can only her/his teachers, counselor and principal see it, or can other teachers and district officials access it? What about individuals or organizations outside the school or district?

IF I WOULD LIKE TO ACCESS AND REVIEW my child's information stored in his or her education records as well as the data in the SIS, as is my right under federal law, how can I do this?

WILL THE SCHOOL INFORM PARENTS when there is a breach of their children's data by the school or district? What methods will be used to inform parents, and how quickly will it happen?

WHEN WILL THE SCHOOL OR DISTRICT DELETE my child's personal data? Once she/he graduates from high school, or if we move? And will all data be deleted or just some of it?
Questions to ask about student information the district shares with the state department of education, the federal government or researchers

EXACTLY WHAT STUDENT INFORMATION is the school or district required to share with the state education department? n IF I WOULD LIKE TO ACCESS AND REVIEW this information for my child, as is my right under federal law, how can I do this?

IF THE SCHOOL OR DISTRICT PARTICIPATES IN A STUDY by independent researchers or the U.S. Department of Education, will they notify parents before sharing personal student information and explain why de-identified or aggregated data are not sufficient for the study?

IF YOU DON'T KNOW the answers to the above questions, who should I ask?

VAFCF
VIRGINIANS FOR Children First

QUESTIONS TO ASK ABOUT YOUR CHILD'S USE OF ONLINE PROGRAMS AND CLASSROOM APPLICATIONS (APPS)

WHICH CLASSROOM APPS and online programs are going to be assigned to my child, and what are their privacy policies?

DO YOU KNOW WHAT INFORMATION VENDORS COLLECT about my child, how it is being used, and with which other third parties or contractors the vendors may be sharing the data?

IS THE VENDOR OR CONTRACTOR ALLOWED to use my child's data for marketing purposes? Will my child see ads as part of the program, or will ads be delivered to my child or to me? If so, how can we opt out of this?
n HAVE THESE PROGRAMS BEEN VETTED by the school, districts, or state for privacy and security? If so, what are the standards for approval?

IF NOT, WHAT ACTIONS HAVE YOU TAKEN TO ENSURE that my child's data will be safe from breach or abuse, and to ensure that these apps comply with state or federal law?

HOW CAN I ACCESS AND REVIEW my child's private information held by these companies and/or request that the information be deleted?

HELPFUL HINT:
The U.S. Department of Education Privacy Technical Assistance Center recommends that schools and/or districts "provide parents with a list of online educational services or 'apps' that are approved for use in the classroom."

HELPFUL HINT:
If your child is under the age of 13, the federal law known as COPPA requires your school to know how the company will use your child's private information before they are allowed to sign up your child to use the classroom app or online program on your behalf. If the company will use your child's private information for any purpose outside of the educational context, the school (or a teacher) may not sign up your child for that classroom app or online program without your permission.

HELPFUL HINT:
Schools or districts that designate companies as "school officials," and then disclose students' personally identifiable information from education records to them, should consider their obligations under the federal law known as FERPA. According to the U.S. Department of Education Privacy Technical Assistance Center: "Whenever a provider maintains a student's education records, the school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access."

WILL THE SCHOOL INFORM PARENTS when there is a breach of student data by a third party or service provider? If we learn of such a breach, what will be done to minimize impacts? Does the vendor have any liability or responsibility to provide credit monitoring or a credit freeze for families who are affected?

QUESTIONS TO ASK ABOUT DATA BREACHES AND ONLINE LEARNING IN GENERAL

HELPFUL HINT:
Also known as a security freeze, a credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves

IF THERE ARE DEFAULT SETTINGS on school-provided devices to collect personal student data, how can the school or I change
those defaults?

WILL MY CHILD'S DATA collected from school-issued devices be de-identified?

WILL THE SCHOOL/DISTRICT or party that provided the school-issued device have remote access to the device? If so, who can access my child's device—the school system administrator, people who work for the software company, administrators, teachers, or more?

CAN EITHER THE PROVIDER or the school turn on the web cam or audio device of a school-issued device? Are they able to remotely access files and documents or view the device screen?

DOES THE SCHOOL have physical or remote access to my child's passwords on the device?

IF I DON'T WANT my child to be monitored and tracked, will my wishes be respected? Can my child still participate in the one-to-one or BYOD program?

[DOES THE SCHOOL use location tracking software to monitor the location of school-issued devices? If so, who can access the location of my child's device and under what circumstances?

DO SPECIAL RULES APPLY if other members of our family use the school-issued device? n WHO IS RESPONSIBLE if the school-issued device breaks or is lost?

HELPFUL HINT:
Schools and districts often use Chromebooks, pre-loaded with Google's G Suite for Education (G Suite), for their 1:1 programs. The Electronic Frontier Foundation recommends changing the Chromebook and G Suite default settings to improve student privacy. Step-by-step instructions can be found at https://www.eff.org/issues/student-privacy/device-settings

HELPFUL HINT:
A Pennsylvania school district admitted that it remotely accessed the webcams of school-issued laptops, secretly taking pictures of students in their own homes. The spying incident prompted the district to pay $61,000 to settle multiple lawsuits.

These questions have been adapted from materials developed by Parents Across America. To learn more, visit www.parentsacrossamerica.org
n HOW MUCH ADDITIONAL TIME, if any, is my child being asked to spend on an electronic device outside of school hours?
n HOW MUCH IS THIS PROGRAM COSTING the school or district?
n IS THE VENDOR PLANNING TO PROFIT by using my child's data for marketing or other commercial purposes?

TALKING TO TEACHERS, SCHOOLS, AND DISTRICTS ABOUT STUDENT PRIVACY

You don't have to be an expert on privacy law or district policies to raise concerns about student privacy. Simply schedule an appointment with your child's teacher or principal and ask some questions to help open the lines of communication. Here are some suggested questions; you do not need to ask them all. You can also follow up with some of the additional questions in Appendix D.

APPROXIMATELY HOW MANY HOURS PER DAY will my child be expected to use an electronic device, including computers, laptops, tablets, and/or smartphones?

WHAT ONLINE PROGRAMS and classroom applications (apps) will my child be assigned to use in class this year?

HAVE THESE PROGRAMS and apps been vetted for data privacy, security, and compliance with state and federal privacy laws?

WHAT DATA IS COLLECTED about my child by the school, its contractors, and any vendors, or operators of online programs and apps used in classrooms?

WHICH OF THIS DATA is being sent to the state department of education?

ARE THE VENDORS supplying these programs barred from using the data for marketing purposes and sharing it with other third
parties, and/or subjecting my child to ads?

HOW CAN I ACCESS the data for my child collected and stored by the vendor or operator, the school, the district, or the state? (See Section II for more information on your rights to access this information under federal law.)

WHO ON THE SCHOOL STAFF and among school contractors, vendors, or operators has access to my child's data?

HOW LONG do the school, contractors, or vendors or operators of online programs and classroom apps retain my child's data?

WHAT DATA does the school or device provider (e.g., Microsoft, Apple, Google, etc.) have access to when my child is using a school- provided device? For example, can the school or device provider access:
ocation information;
• IP addresses;
• camera and microphone;
• browsing history;
• locally stored content; • contacts; or
• anything else not explicitly provided to the school by my c

U.S. Department of Education

Student Privacy Policy Office

Local Education Agency Website Student Privacy Transparency Reviews – Combined Two-Year Report Summary

Review Period: September 2018-April 2020

Executive Summary

The Student Privacy Policy Office (SPPO) at the U.S. Department of Education (Department) is performing a four-year review of a sample of the websites of 1,504 local education agencies (LEAs) to identify whether and how these websites include information about student privacy. In each year of the study, SPPO is reviewing a nationally representative sample of 376 LEA websites, focusing on whether the LEAs included key student privacy documents and information about the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA) on the LEA website, as opposed to on individual school, board of education, or other websites. This report includes the first two years of research findings.

Combined two-year findings:

- 54 percent of LEAs reviewed posted on their websites the LEA's Annual Notice under FERPA,
- 52 percent of LEAs posted on their websites the LEA's policy under the Directory Information exception under FERPA, and
- 29 percent of LEAs posted on their website the LEA's policy under PPRA.

For these three key privacy documents that are posted on the LEA websites, fewer than twenty percent are listed as primary website content. In more than fifty percent of the cases, the documents are included as part of the student handbook, which may be a Portable Document Format (PDF) or other type of document linked from the LEA webpage.

For the websites reviewed, 12 percent of LEA websites have navigation menus that include a section indicating where to find data practices and student privacy information. Moreover, only 7 percent of LEA websites include the LEA contact information if parents have questions about data sharing and student privacy.

UNITED STATES DEPARTMENT OF EDUCATION

STUDENT PRIVACY POLICY OFFICE

November 1, 2021

Letter to State Superintendent

CLICK HERE

Dear Chief State School Officers and Superintendents:

The Student Privacy Policy Office (SPPO) at the U.S. Department of Education (Department) provides annual notification to State educational agencies (SEAs) and local educational agencies (LEAs) regarding the educational agencies' obligations under the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) and the Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h; 34 CFR Part 98). The annual notification, which is required by 20 U.S.C. § 1232h(c)(5)(C), has not substantively changed since it was last issued. The notification may be accessed via our website at https://studentprivacy.ed.gov/annual-notices.

FERPA and PPRA

FERPA is a Federal law that protects the privacy rights of parents and students in education records maintained by educational agencies and institutions or by persons acting for such agencies or institutions. PPRA affords parents and students with rights concerning certain SEA and LEA marketing activities, the administration or distribution of certain surveys to students, the administration of certain physical examinations or screenings to students, and parental access to certain instructional materials. Resources on FERPA and PPRA, including SPPO's online FERPA training modules, our technical assistance request process, and our complaint process, can be accessed on our website at https://studentprivacy.ed.gov/. We also recommend that you sign up for our periodic student privacy newsletter by visiting https://studentprivacy.ed.gov/join-student-privacy-listserv.

SPPO Resources

In addition to SPPO's general resources, we want to highlight the following specific resources that may be helpful.

Resources on FERPA, COVID-19, and virtual learning:

- *FERPA and Virtual Learning During COVID-19*; *FERPA and the Coronavirus Disease 2019 (COVID-19) FAQs*; and *May Schools Disclose Information about Cases of COVID-19?* – provide information on the applicability of FERPA to COVID-19 related disclosures.
  https://studentprivacy.ed.gov/covid-19

Letter to your local Superintendent

UNITED STATES DEPARTMENT OF EDUCATION

STUDENT PRIVACY POLICY OFFICE

April 2020

The Family Educational Rights and Privacy Act (FERPA)

Statute: 20 U.S.C. 1232g. Regulations: 34 CFR Part 99.

CLICK HERE

Rights of Parents

FERPA provides that a local educational agency (LEA) that receives Department of Education (Department) funds may not have a policy or practice of denying parents the right to:

- Inspect and review education records within 45 days of a request (§ 99.10);
- Seek to amend education records believed to be inaccurate (§§ 99.20, 99.21, and 99.22); and
- Consent to the disclosure of personally identifiable information (PII) from education records except as specified by law (§§ 99.30 and 99.31).

These rights transfer to the student when he or she turns 18 years of age or enters a postsecondary educational institution at any age ("eligible student"). The Student Privacy Policy Office (SPPO) in the Department, the office that administers FERPA, has issued guidance documents about FERPA for parents and for eligible students. Those documents are available on SPPO'S website at:
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/for-parents.pdf and
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/for-eligible-students.pdf.

FERPA Regulations

The FERPA regulations can be found on SPPO's website at this link: https://studentprivacy.ed.gov/node/548/. We last made changes to the regulations in 2011. You can view the *Federal Register* notice for those amendments to FERPA at http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf.

Statutory Amendments to FERPA Not in Regulations

There are two statutory amendments that Congress has made to FERPA that are not yet in the regulations. These amendments are described below:

Uninterrupted Scholars Act of 2013: In January 2013, Congress passed the "Uninterrupted Scholars Act (USA)" which amended FERPA to permit educational agencies and institutions to disclose personally identifiable information from education records of a student in foster care placement to an agency caseworker or other representative of a State or local child welfare agency or tribal organization who is authorized to access a student's case plan when such agency or organization is legally responsible, in accordance with State or tribal law, for the care and protection of the student. See 20 U.S.C. 1232g(b)(1)(L). The USA also amended the exception

FAIRFAX- only VA county to get this right??

NOTIFICATION OF TESTING
Social and Emotional Learning (SEL) Screener

Dear Parents and Guardians:

Fairfax County Public Schools (FCPS) commits to supporting all students' mental wellness and social and emotional learning (SEL). The School Board has approved a screener to review students' skills and experiences in these areas. FCPS staff will use the screener to identify strengths and needs for students in grades K-12. The screener provides information regarding students' experiences and how staff can support their needs.

SEL skills include self-awareness, self-management, social awareness, relationship skills, and responsible decision-making. The screener will review these skills, as well as students' relationships, feelings of belonging, feelings about their school environment, and mood. These factors are critical to positive academic, social, and emotional success.

Students in grades K-2 will be screened in the winter and spring. In these grade levels, teachers will complete a survey on their observations of students' skills and experiences. Students in grades 3-12 will be screened in the fall, winter, and spring. In these grade levels, students will reflect and report on their own skills and experiences. Screener data will only be accessible to teachers, administrators, and staff with legitimate educational interests. Results will be maintained in secure files and databases accessible only to these individuals. Screener results will be used with other data to inform practices for SEL skill development and mental wellness. Screener data will also help staff plan interventions for students with identified needs. Parents and guardians will receive an individualized report regarding their student's screener results following each assessment window. School staff will be available to discuss results with families on planned support.

Schools will set specific dates for testing in each class. If you do not want your student to take part in the SEL screener, please return the opt-out form below to the school.

More information, including a short video about the SEL screener in FCPS and the screener questions, can be found on the SEL Screener webpage (https://www.fcps.edu/node/43892). Please contact your student's school counselor or the school's test coordinator with questions.

Fairfax County Social Emotional Learning Screener- OPT-OUT REQUEST FORM

If you wish to opt your child out of participating in the SEL Screener, please complete this form and return it to your child's teacher by _____.

PLEASE NOTE: You do not need to return this form unless you do not want your child to participate in the SEL screener this year.

CHILD'S NAME_____**TEACHER**_____

Parent/Guardian Signature_____ **Date**_____

For a translation of this document, please visit the webpage at https://www.fcps.edu/node/43941 or contact your student's school.
لغرض الأطلاع على ترجمة هذه الوثيقة، يرجى زيارة الموقع الألكتروني https://www.fcps.edu/node/43941 أو الأتصال بمدرسة الطالب.
如果您需要本文件的翻译文本，请访问网页 https://www.fcps.edu/node/43941 或联系您的学生所在学校。
برای دسترسی به ترجمه این سند ، لطفاً به وب سایت https://www.fcps.edu/node/43941 مراجعه کنید و یا با مدرسه دانش آموز خود تماس بگیرید.
이 문서의 번역은 웹페이지, https://www.fcps.edu/node/43941 를 방문하거나 자녀의 학교에 문의하시기 바랍니다.
Para obtener la traducción de este documento, sírvanse ir a la página web https://www.fcps.edu/node/43941 o contactar a la escuela de su hijo(a).
اس دستاویز کے ترجمے کے لیئے، براہ مہربانی https://www.fcps.edu/node/43941 کے ویب پیج پر تشریف لے جائیں یا اپنے بچے کے اسکول سے رابطہ کریں۔
Để có bản dịch của tài liệu này, xin vui lòng truy cập trang mạng tại https://www.fcps.edu/node/43941 hoặc liên lạc với trường của con em quý vị.

BURBANK SCHOOL DISTRICT 111

DISTRICT OFFICE
7600 S. Central Avenue
Burbank, Illinois 60459
Telephone: (708) 496-0500
Fax: (708) 496-0510

DISTRICT 111 SCHOOLS
K-6 Elementary Schools
Luther Burbank
8235 S. Linder
Telephone: (708) 499-0838
Fax: (708) 499-0502

Richard E. Byrd
8259 S. Lavergne
Telephone: (708) 499-3049
Fax: (708) 499-1002

Harry E. Fry
7805 S. Mobile
Telephone: (708) 599-5554
Fax: (708) 599-1348

Jacqueline B. Kennedy
7644 S. Central
Telephone: (708) 496-0563
Fax: (708) 496-8365

Rosa G. Maddock
8258 S. Sayre
Telephone: (708) 598-0515
Fax: (708) 233-6401

Frances B. McCord
8450 S. Nashville
Telephone: (708) 599-4411
Fax: (708) 233-9104

Edward J. Tobin
8501 S. Narragansett
Telephone: (708) 599-6655
Fax: (708) 233-9014

Junior High School
Liberty Junior High
5900 West 81st Street
Telephone: (708) 952-3255
Fax: (708) 229-0659

March, 2022

Dear Parents and Guardians,

We are thrilled to let you know Burbank School District 111 is focused on supporting your child's social-emotional needs! Over two decades of research has shown the important roles social and emotional skills play in each child's success in school and the community. Skills such as demonstrating self-control, persisting at challenging tasks, and making good decisions are all necessary to being successful students and adults. The process by which students learn these and other similar skills is called social and emotional learning (SEL).

As part of this initiative, teachers will be completing a short 8 question tool called the Devereux Student Strengths Assessment, or DESSA-mini. This tool asks how often a child has demonstrated specific social and emotional skills in the past month.

Some sample DESSA questions include:
- How often did the child keep trying when unsuccessful?
- How often did the child offer to help somebody?
- How often did the child work well in groups?

The purpose of the DESSA is to identify which SEL skills your child has already learned and what skills he or she might still need to develop. Once our teachers identify the skills their students still need to learn, they will teach those SEL skills. Our goal is to ensure that your child is continuously developing the SEL skills that they need for lifelong success. We believe that the information gathered from the DESSA will be beneficial to your child's overall success both inside and outside of the classroom

The DESSA is published by Aperture Education. Our district chose the DESSA in part because of Aperture Education's strong commitment to respecting and protecting your child's privacy. We also chose Aperture Education because they offer a Family Resources page on their website that provides resources, tips, and strategies to parents on supporting their child's social and emotional development. To view additional information about the DESSA, the privacy policy, or our Family Resources page, visit www.ApertureEd.com.

Students will be screened using the DESSA mini-screener on March 15, 2022. Teachers will be screening the students based on classroom observation. If you prefer your student not be screened, please return this letter to your classroom teacher no later than Monday, March 14, 2022.

We are excited to implement the DESSA! If you have any questions, please feel free to email me at dflavin@bsd111.org.

Sincerely,

Denise M Flavin

Denise M Flavin
Director of Curriculum and Instruction

_____ I do not want my student, _____ social emotionally screened using the DESSA screener. (student's name)

Department of Education
Chancellor Richard A. Carranza

Intermediate School 349
The School of Math, Science and Technology
35 Starr Street Brooklyn, New York 11221
Phone (718) 418-6389 Fax (332) 900-8485

IS 349
THE SCHOOL OF MATHEMATICS SCIENCE AND TECHNOLOGY

November 10, 2021

Dear Parent(s)/Guardian(s),

We understand just how challenging the past 18 months of the pandemic have been for you as parents, families, and caregivers. We are in awe of the work you have done, and continue to do each and every day, to support your child(ren) and we thank you for your continued partnership with us. Our work together is more important than ever as we strive to ensure your child thrives this school year and beyond. To further support you, our teachers, counselors, and social workers as champions of your child(ren)'s academic and social and emotional needs, are excited to let you know about a wonderful opportunity in our school this year!

Research has consistently shown that developing the social and emotional skills of students helps them to succeed academically, gain confidence, and be happier. Social-emotional learning, or SEL, includes developing relationship skills, self-awareness, responsible decision-making, and optimistic thinking.

To identify and support the social-emotional growth of all children in our school, we are excited to be administering a strengths-based SEL screener, known as the Devereaux Student Strengths Assessment (DESSA). The DESSA asks questions about areas of social-emotional functioning including decision making, relationship building, confidence, and others. This tool will be completed by someone who knows your child really well—in most cases a teacher.

The responses we gather will help us provide targeted, highly responsive support to each individual student. Perhaps most importantly, the tool enables us to build on each student's strengths while identifying the social-emotional skills they need to further develop. Once our students' growth areas are identified, we can create highly responsive plans to target and enhance those skills in the most appropriate manner and settings.

The results of this screener will not be included on report cards, will not have any impact on grades, and will not be used to make any diagnostic or evaluation decisions. The results will be stored securely in an online portal that meets the DOE's strictest privacy and security settings and will only be viewable by your child(ren)'s teachers and select school staff such as the principal or counselor.

The information gathered from the DESSA screening tool will allow us to provide the very best support to your child and will be beneficial to their overall success, both inside and outside of school. Families will have an opportunity to hear about their student's SEL skills during family conferences.

We are excited to implement the DESSA beginning Tuesday, November 16, 2021. If you have any questions, please feel free to call the main office at 718-418-6389.

If you do not want a staff member to complete the DESSA screener for your student, you must write a letter to me stating that. This letter needs to be received by the school by Monday, November 15, 2021.

If you have any questions regarding social-emotional learning or the DESSA, please email me Ms. Toro-Ruiz at RToro6@schools.nyc.gov.

Sincerely,

Roxana Toro-Ruiz, Principal

Fairfax County PUBLIC SCHOOLS
ENGAGE • INSPIRE • THRIVE

Lees Corner Elementary School
13500 Hollinger Avenue
Fairfax, Virginia 22033

Dear Parents/Guardians,

Fairfax County Public Schools uses a variety of resources to support student learning. Some of the digital resources your child may use this year require parental consent according to their terms of service and/or privacy policy. FCPS takes your child's privacy and security very seriously, and follows the guidelines set forth by federal legislation.[1] The tools listed below have been thoroughly reviewed and approved for use in FCPS.

• Class Dojo • Code.org • duoLingo • EDPuzzle	• FlipGrid • Flocabulary • goFormative • Khan Academy	• Newsela • NoRedInk (Free Version) • Padlet	• Quizlet • Remind • Vocabulary.com • Wizer.me

A more detailed explanation of each of the tools can be found on the attached page. After reviewing terms of service and/or privacy policies for each of the digital resources listed on this document, please sign and return page one of this form to your child's homeroom teacher. You may keep the remaining pages for future reference.

Additional parent consent letters for other FCPS approved digital resources will be sent home by your child's teacher prior to using them with students on an as needed basis.

Student First and Last Name	
Teacher's Last Name	
Parent First and Last Name	
Signature of Parent / Guardian	
Date	

Students are instructed to use their FCPS Google account to log in to each of these resources.

Thank you,
Your Child's Teacher

[1] Federal guidelines regarding online safety for children include:
Family Educational Rights and Privacy Act (FERPA)
Children's Online Privacy and Protection Act (COPPA)
Children's Internet Protection Act (CIPA)

Tool	Purpose	Terms of Service and Privacy Policy
ClassDojo	A communication app for the classroom. It connects teachers, parents, and students who use it to share photos, videos, and messages through the school day.	https://www.classdojo.com/terms/ https://www.classdojo.com/privacy/
CODE.org	Learn the basic concepts of Computer Science with drag and drop programming.	https://code.org/tos https://code.org/privacy
duolingo	Tool for learning language through interactive activities.	https://www.duolingo.com/terms https://www.duolingo.com/privacy
EDpuzzle	Teachers and students can annotate videos and create interactive videos for instruction.	https://edpuzzle.com/terms https://edpuzzle.com/privacy
FLIPGRID.	A video discussion community for your classroom that supercharges your students' voices.	https://legal.flipgrid.com/ https://info.flipgrid.com/
Flocabulary	A web-based learning program for all grades and subjects that uses hip-hop to engage students in vocabulary instruction.	https://www.flocabulary.com/terms-of-use/ https://www.flocabulary.com/privacy-policy/
formative	Activities that check for student understanding.	https://goformative.com/tos https://goformative.com/privacy
KHANACADEMY	Resource for learning through videos and practice exercises.	https://www.khanacademy.org/about/tos https://www.khanacademy.org/about/privacy-policy
NEWSELA	Nonfiction articles and current events at various reading levels.	https://newsela.com/pages/terms-of-use/ https://newsela.com/pages/privacy-policy/

padlet	Virtual bulletin board for collaborating and creating.	https://padlet.com/about/terms https://padlet.com/about/privacy
Quizlet | Q	A study tool for matching terms and definitions.	https://quizlet.com/tos https://quizlet.com/privacy
remind	A communication service for sending reminders from the teacher to parents and students.	https://www.remind.com/terms-of-service https://www.remind.com/privacy-policy
noredink	A web-based learning platform that helps students improve their grammar and writing skills.	https://www.noredink.com/terms https://www.noredink.com/privacy
Vocabulary.com	A vocabulary study resource.	https://www.vocabulary.com/terms/ https://www.vocabulary.com/privacy/
wizer.me	Allows teachers to combine video, audio, images, and checks for understanding, to create an interactive set of online activities for instruction.	https://app.wizer.me/tos https://app.wizer.me/privacy


DATA
VAFCF
VIRGINIANS FOR Children First
What you are not changing, you are choosing
WWW.VIRGINIANSFORCHILDRENFIRST.ORG
GET EDUCATED!!
LEGAL FUND