How to use the

Parent Toolkit for Student Privacy

Presentation to CPAC June 1, 2017

PARENT COALITION FOR STUDENT PRIVACY

Who developed the toolkit

PARENT COALITION FOR
STUDENT PRIVACY

The Parent Coalition for Student Privacy is a national grassroots advocacy group formed in 2014 to help parents defend the rights of parents and students to protect their personal information at school. PCSP is a project of Class Size Matters, a 501C3 nonprofit.

http://www.studentprivacymatters.org/

ccfc
Campaign for a Commercial-Free Childhood

CCFC's mission is to support parents' efforts to raise healthy families by limiting commercial access to children and ending the exploitive practice of child-targeted marketing. In working for the rights of children to grow up—and the freedom for parents to raise them—without being undermined by corporate interests, CCFC promotes a more democratic and sustainable world.

http://www.commercialfreechildhood.org/

Why is student privacy so important?

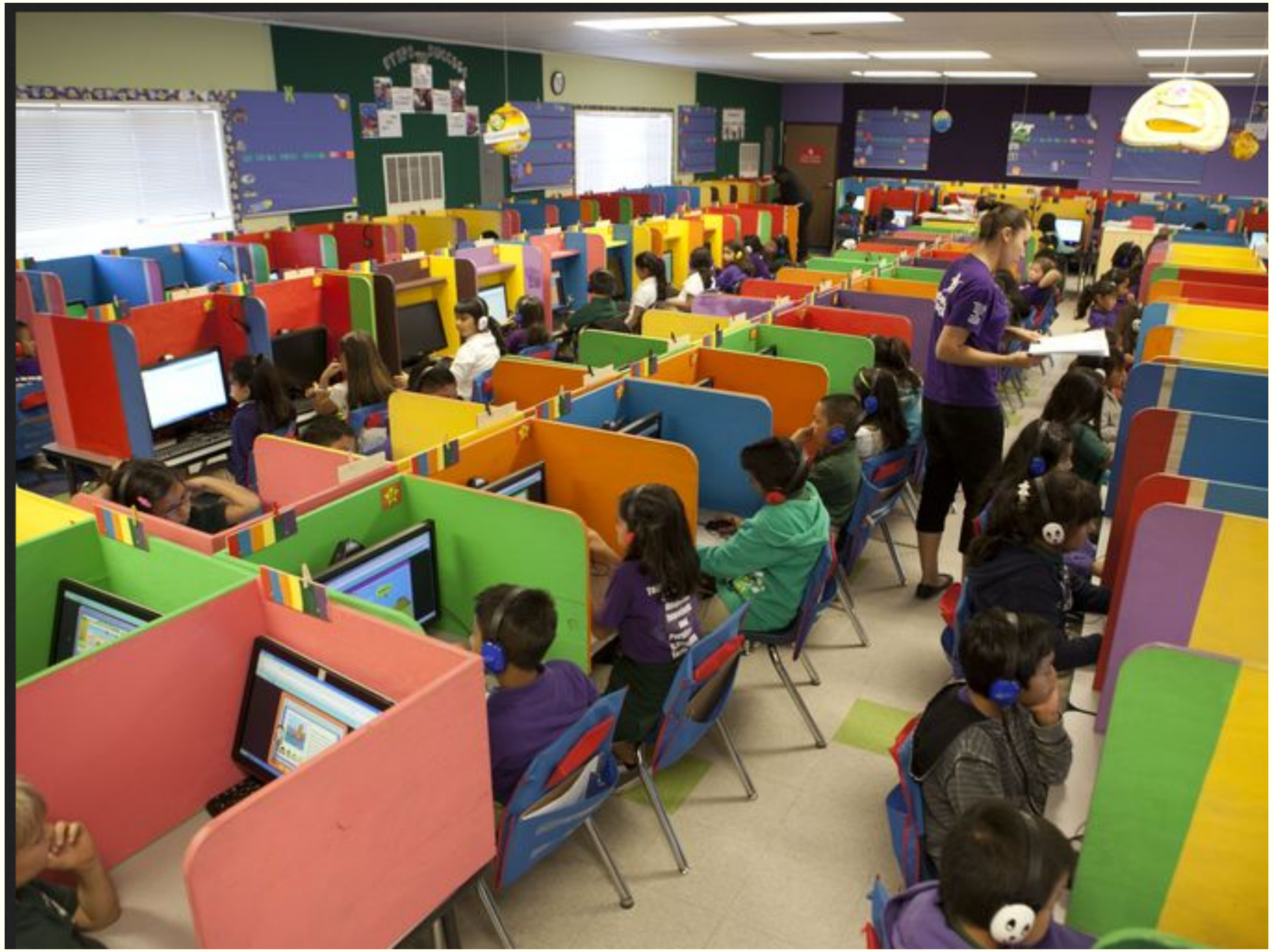
Why is student privacy so important?

- Huge push by ed tech industry, government, foundations, advocacy groups to promote outsourcing school operations, instruction, assessment and behavior management to private for-profit vendors and other third parties

- This effort depends on private vendors being able to access and data mine large amounts of personal student info --- including in many cases their names, test scores, grades, disabilities, disciplinary records, economic & racial status and more .

- To facilitate transfer of data, US Dept of Ed has weakened student privacy laws to no longer require parental notification and consent before schools share personal student info with 3rd parties outside school or district.

“Personalized learning” according to corporate reformers



How does this endanger student privacy?

- In some cases, schools and districts are being offered classroom apps for free – but at the cost of monetizing their students' personal data
- There are NO security requirements for storing or transmitted personal student data in FERPA or other federal laws–
- As a result, we have seen increasing numbers of breaches by districts, schools and for-profit vendors
- In last few weeks alone EdModo and Schoolzilla – both popular educational apps – have suffered breaches, putting personal info of millions of students – and parents -- at risk

What about inBloom?

- In 2012 we heard about the Shared Learning Collaborative, a mega-project project of Gates Foundation created with over $100M .
- Designed to collect, systematize, and store personal student data & share with for-profit vendors to make education more “efficient”
- SLC spun off as a separate corporation in March 2013 called inBloom Inc.
- We blogged about inBloom, to alert parents in the 9 states and districts that had promised to share student data
- Within 13 months of launch, because of fierce parent opposition, every state & district pulled out and inBloom collapsed.
- July 2014 we formed Parent Coalition for Student Privacy with other parents to work towards stronger student privacy laws and practices.

What did we learn from the inBloom experience?

- inBloom tip of the iceberg. Data-mining software companies see huge potential & profit in putting education/assessment online.

- Education tech market estimated at more than $7.9 *billion*, over $90 billion globally – with the ultimate goal to eliminate the need for human teachers as possible in favor of computers and software.

- ***But we also learned from defeating inBloom that parents can be very powerful, if have information and right advocacy tools to resist and protect their children's privacy.***

- This is just what our toolkit was designed to do – to empower parents through alerting them to their rights and also how to advocate for strong privacy protections with their schools and districts.

What else have we learned?

MANY schools and districts violate federal student privacy laws, including FERPA, Family Education Rights and Privacy Act, passed in 1974.

Example: Data walls in classrooms ***violate FERPA*** if they contain student personally identifying info along with test scores or grades

Free lunch lines in schools violate the NSLA (National School Lunch Act) passed in 1946

A student's eligibility info for free lunch or reduced price lunch CANNOT be made available to all school employees, or to other students – only those officials directly involved in their education.

Overt identification of free or reduced lunch students is prohibited by having separate dining areas, serving lines, different color-coded tickets or IDs or any practice that would overtly identify these students.

Laws on sharing Directory Info – does DOE comply?

- Every year, schools and districts are supposed to tell parents they have the right to opt out of directory information being shared with vendors or other organizations who do NOT have contracts or agreements with the district for operational or research purposes.

- Directory info can include ***student and/or parent names, addresses, email addresses, grade level, enrollment status, honors and awards received, and the most recent school attended.***

- DOE currently provides much of this info to mailing houses who are paid by charter schools to recruit students

- However many parents say they have NOT been informed of the right to opt out of these disclosures.

- The DOE also chooses not to give same information free of charge to CECs – though they could choose to do so. Instead they require that CECs hire these mailing houses for a fee.

What’s in the Parent Toolkit for Student Privacy?

The Parent Toolkit for Student Privacy

Introduction: Why should parents be concerned?

Table of Contents

Section I: What is student data?

Section II: Parents' rights under federal law to protect their children's privacy

Section III: Tips for parents looking to protect their children's privacy

Section IV: Student privacy best practices for states, districts, schools, and teachers

Section V: Talking to teachers, schools, and districts about student privacy

Section VI: Advocating for student privacy in schools, districts, and beyond

Section VII: Student privacy FAQs

Appendix A: Request to inspect education records held by the school, district or state

Appendix B: Sample letter to opt out of disclosure of directory information

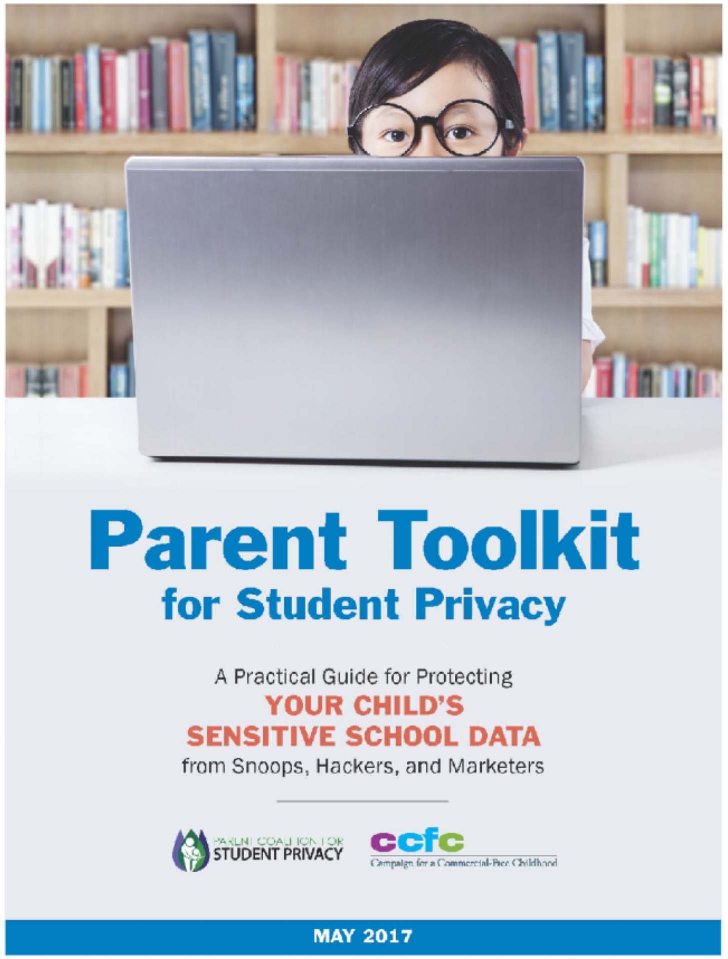
Appendix C: Sample letter to opt out of military recruitment

Appendix D: Additional questions to ask your teacher or principal

Appendix E: Sample petition

Appendix F: Tips for media outreach and sample press materials

Additional resources



Parent Toolkit
for Student Privacy

A Practical Guide for Protecting
YOUR CHILD'S
SENSITIVE SCHOOL DATA
from Snoops, Hackers, and Marketers

PARENT COALITION FOR STUDENT PRIVACY

ccfc
Campaign for a Commercial-Free Childhood

MAY 2017

www.studentprivacymatters.org/toolkit

Parent Toolkit for Student Privacy: Section I

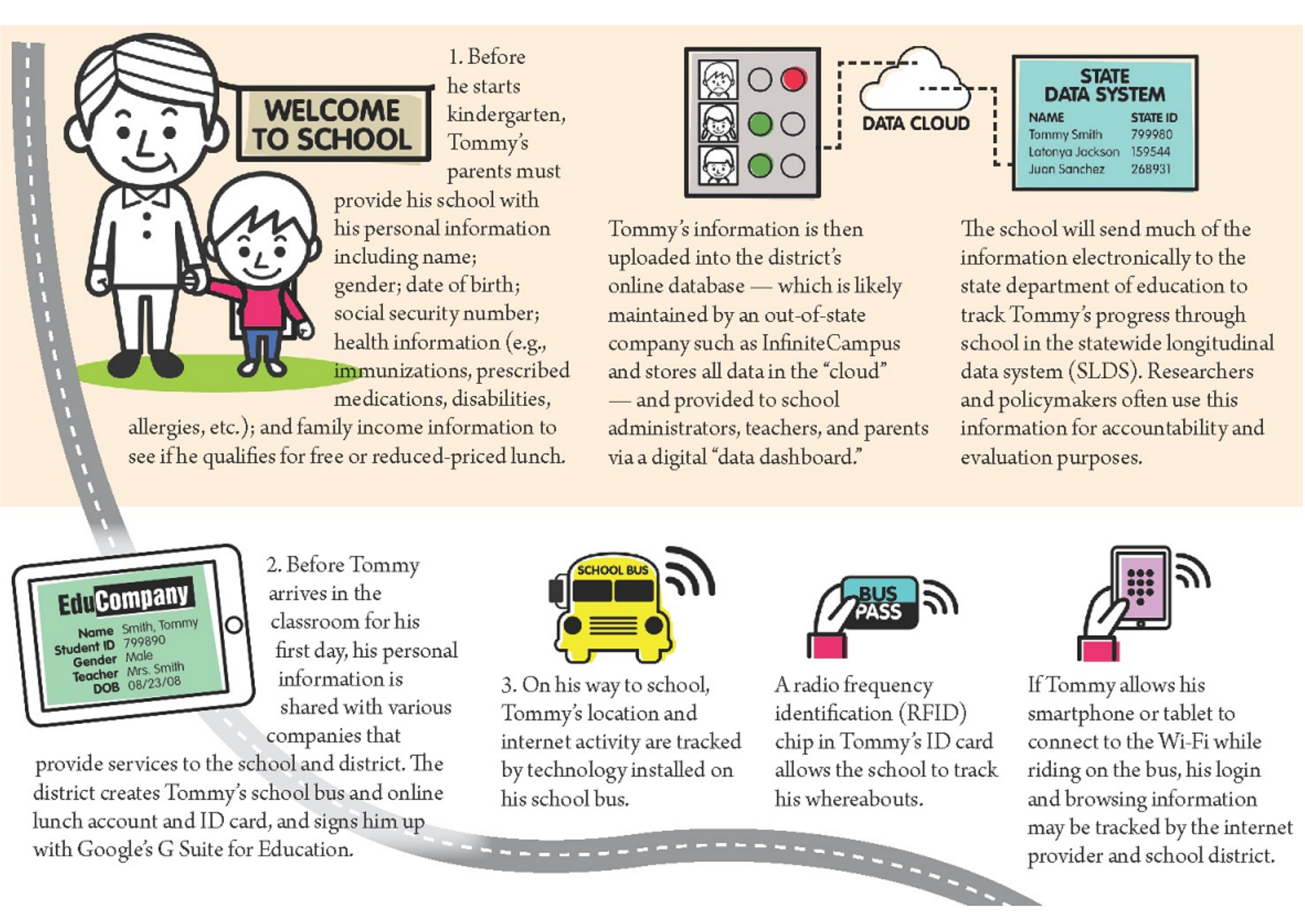
What is student data?

- "Tommy" infographic describes the types and volume of student data collected

- Gives examples of how the data is currently used/shared and can be used/shared in the future

How to use this section:

Connect the dots to what's happening in your child's classroom and share with others.



1. Before he starts kindergarten, Tommy's parents must provide his school with his personal information including name; gender; date of birth; social security number; health information (e.g., immunizations, prescribed medications, disabilities, allergies, etc.); and family income information to see if he qualifies for free or reduced-priced lunch.

Tommy's information is then uploaded into the district's online database — which is likely maintained by an out-of-state company such as InfiniteCampus and stores all data in the "cloud" — and provided to school administrators, teachers, and parents via a digital "data dashboard."

The school will send much of the information electronically to the state department of education to track Tommy's progress through school in the statewide longitudinal data system (SLDS). Researchers and policymakers often use this information for accountability and evaluation purposes.

2. Before Tommy arrives in the classroom for his first day, his personal information is shared with various companies that provide services to the school and district. The district creates Tommy's school bus and online lunch account and ID card, and signs him up with Google's G Suite for Education.

3. On his way to school, Tommy's location and internet activity are tracked by technology installed on his school bus.

A radio frequency identification (RFID) chip in Tommy's ID card allows the school to track his whereabouts.

If Tommy allows his smartphone or tablet to connect to the Wi-Fi while riding on the bus, his login and browsing information may be tracked by the internet provider and school district.

Parent Toolkit for Student Privacy: Section II

Parents’ rights under federal law to protect their children’s privacy

- Easy-to-understand descriptions of parents’ rights and instructions on how to file complaints
- **FERPA** – protects education records collected & maintained by schools (and some of their vendors)
- **IDEA** – protects the rights of children with disabilities
- **NSLA** – protects confidential eligibility and income information used by schools to determine whether a child qualifies for FRL
- **PPRA** – applies to student surveys relating to sensitive issues; includes protections regarding marketing, parental access to instructional materials, and some physical examinations
- **COPPA** – gives parents some control over information collected online directly from children under 13 years old.

FERPA (Family Education Rights and Privacy Act)

IDEA (Individuals with Disabilities Education Act)

NSLA (National School Lunch Act)

Questionnaire

PPRA (Protection of Pupil Rights Amendment)

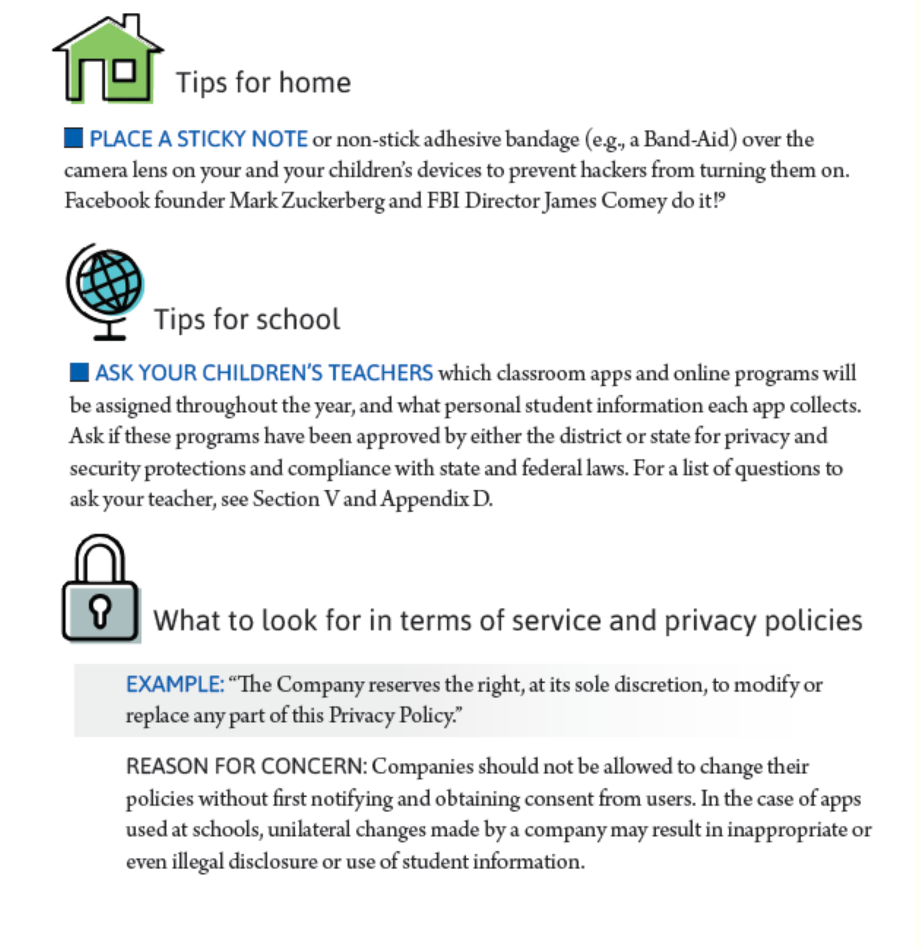
COPPA (Children’s Online Privacy Protection Act)

Parent Toolkit for Student Privacy: Section III

Tips for parents looking to protect their student's privacy

- Simple, practical tips to protect your child's privacy at home and at school

- Gives examples of red flags to look for in terms of service and privacy policies



Tips for home

■ PLACE A STICKY NOTE or non-stick adhesive bandage (e.g., a Band-Aid) over the camera lens on your and your children's devices to prevent hackers from turning them on. Facebook founder Mark Zuckerberg and FBI Director James Comey do it![9]

Tips for school

■ ASK YOUR CHILDREN'S TEACHERS which classroom apps and online programs will be assigned throughout the year, and what personal student information each app collects. Ask if these programs have been approved by either the district or state for privacy and security protections and compliance with state and federal laws. For a list of questions to ask your teacher, see Section V and Appendix D.

What to look for in terms of service and privacy policies

EXAMPLE: "The Company reserves the right, at its sole discretion, to modify or replace any part of this Privacy Policy."

REASON FOR CONCERN: Companies should not be allowed to change their policies without first notifying and obtaining consent from users. In the case of apps used at schools, unilateral changes made by a company may result in inappropriate or even illegal disclosure or use of student information.

Parent Toolkit for Student Privacy: Section IV

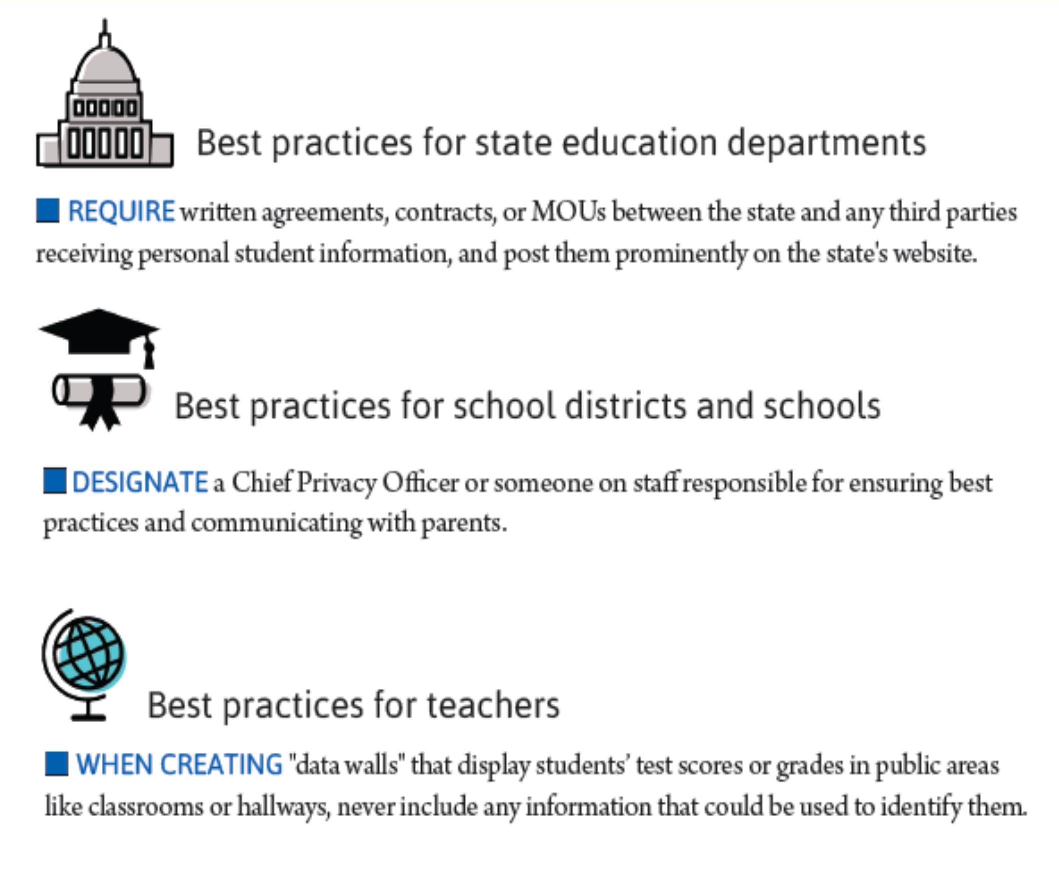
Privacy best practices for states, districts, schools, and teachers

- Incorporates recommendations from the US Dept. of Education, Fordham Law School, Parent Coalition's Five Principles to Protect Student Privacy , and others

- Gives technical guidance on good policy-making to protect student privacy

How to use this section:

Share with teachers, school administrators, DOE and NYSED



Best practices for state education departments

■ REQUIRE written agreements, contracts, or MOUs between the state and any third parties receiving personal student information, and post them prominently on the state's website.

Best practices for school districts and schools

■ DESIGNATE a Chief Privacy Officer or someone on staff responsible for ensuring best practices and communicating with parents.

Best practices for teachers

■ WHEN CREATING "data walls" that display students' test scores or grades in public areas like classrooms or hallways, never include any information that could be used to identify them.

Parent Toolkit for Student Privacy: Section V

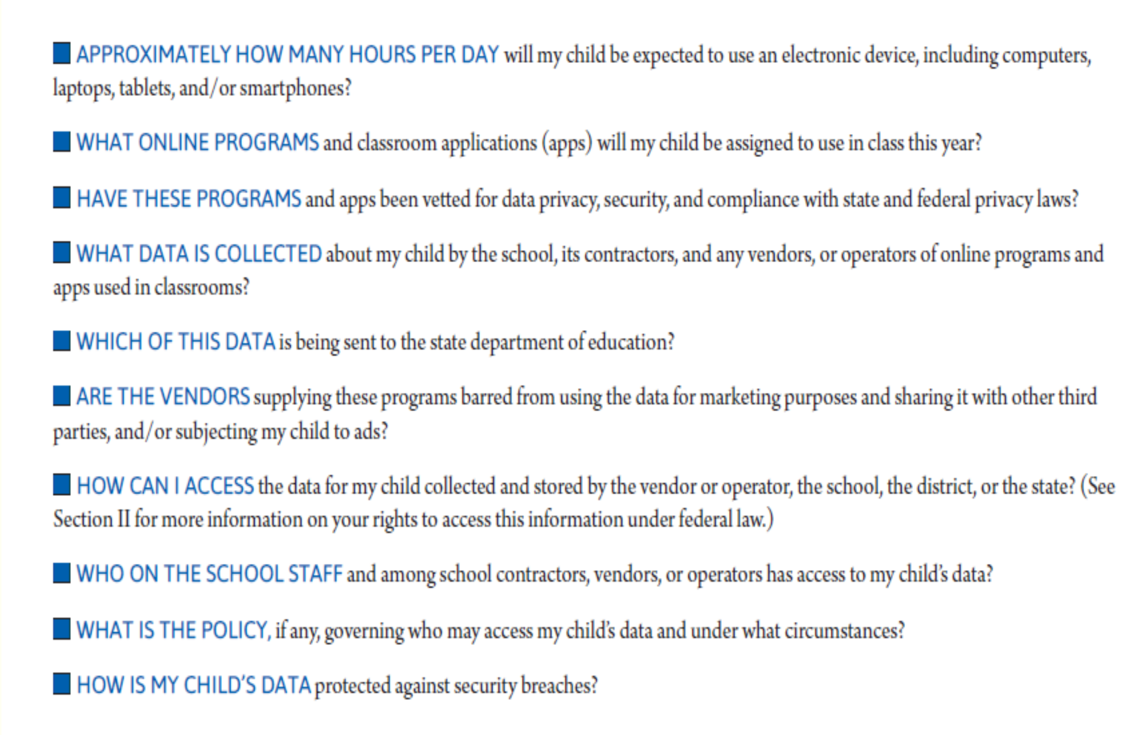
Talking to teachers, schools and districts about student privacy

- Non-confrontational questions to ask about the use of technology at school

- Follow-up questions about how student data is used and protected

How to use this section:

Share with your teachers or principal during back-to-school night or at parent-teacher conferences.



- 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?
- WHAT IS THE POLICY, if any, governing who may access my child's data and under what circumstances?
- HOW IS MY CHILD'S DATA protected against security breaches?

Parent Toolkit for Student Privacy: Section VI

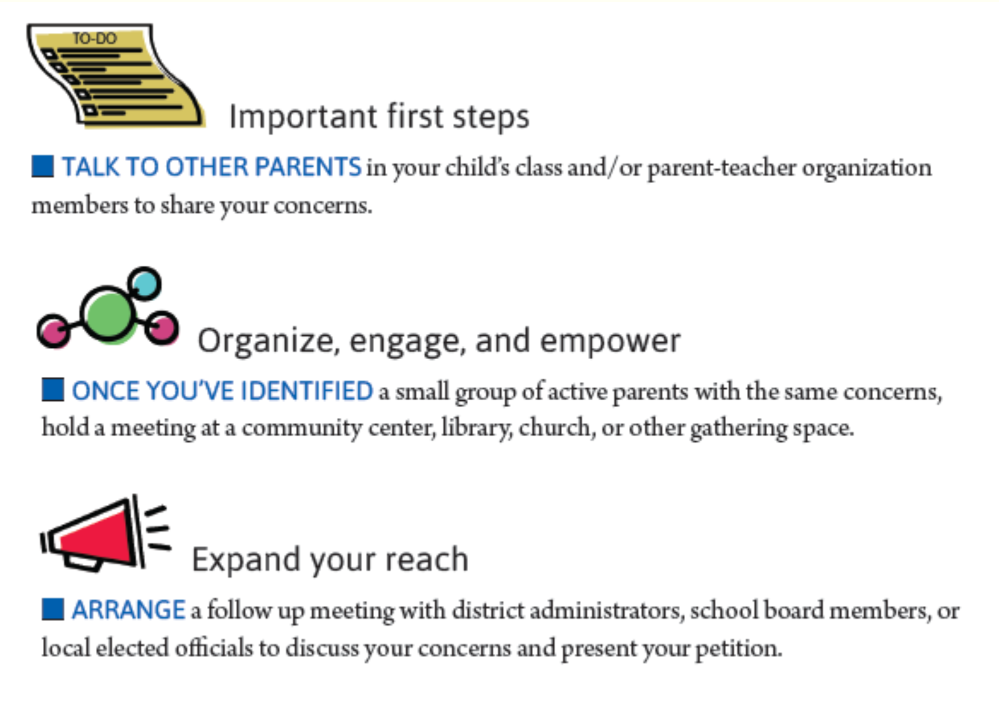
Advocating for student privacy in schools, districts, and beyond

- Step-by-step instructions for building grassroots support

- Includes helpful tips for getting media attention and writing letters to the editor

How to use this section:

If you're dissatisfied with your school's response to questions in Section V, use this section to convert your concern into action.



Important first steps

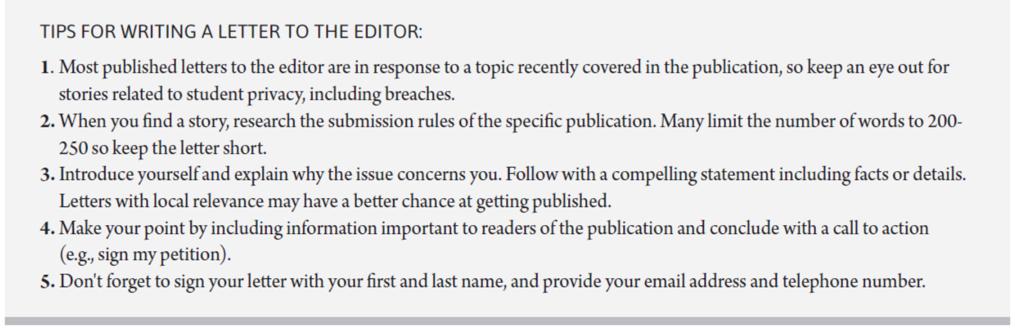
■ TALK TO OTHER PARENTS in your child's class and/or parent-teacher organization members to share your concerns.

Organize, engage, and empower

■ ONCE YOU'VE IDENTIFIED a small group of active parents with the same concerns, hold a meeting at a community center, library, church, or other gathering space.

Expand your reach

■ ARRANGE a follow up meeting with district administrators, school board members, or local elected officials to discuss your concerns and present your petition.



TIPS FOR WRITING A LETTER TO THE EDITOR:

1. Most published letters to the editor are in response to a topic recently covered in the publication, so keep an eye out for stories related to student privacy, including breaches.
2. When you find a story, research the submission rules of the specific publication. Many limit the number of words to 200-250 so keep the letter short.
3. Introduce yourself and explain why the issue concerns you. Follow with a compelling statement including facts or details. Letters with local relevance may have a better chance at getting published.
4. Make your point by including information important to readers of the publication and conclude with a call to action (e.g., sign my petition).
5. Don't forget to sign your letter with your first and last name, and provide your email address and telephone number.

Parent Toolkit for Student Privacy: Section VII

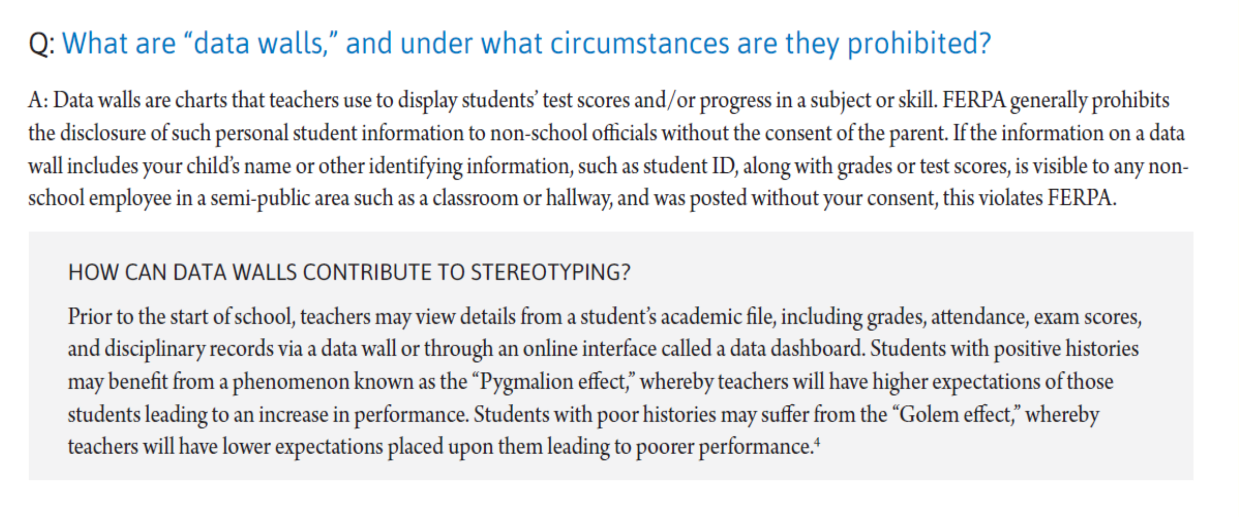
Student privacy FAQs

- Answers to the most common questions about student privacy

How to use this section:

Check out this section when you have specific questions you need answered. Shoot us an email if you can't find what you're looking for!

info@studentprivacymatters.org



Q: What are "data walls," and under what circumstances are they prohibited?

A: Data walls are charts that teachers use to display students' test scores and/or progress in a subject or skill. FERPA generally prohibits the disclosure of such personal student information to non-school officials without the consent of the parent. If the information on a data wall includes your child's name or other identifying information, such as student ID, along with grades or test scores, is visible to any non-school employee in a semi-public area such as a classroom or hallway, and was posted without your consent, this violates FERPA.

HOW CAN DATA WALLS CONTRIBUTE TO STEREOTYPING?

Prior to the start of school, teachers may view details from a student's academic file, including grades, attendance, exam scores, and disciplinary records via a data wall or through an online interface called a data dashboard. Students with positive histories may benefit from a phenomenon known as the "Pygmalion effect," whereby teachers will have higher expectations of those students leading to an increase in performance. Students with poor histories may suffer from the "Golem effect," whereby teachers will have lower expectations placed upon them leading to poorer performance.[4]

How can I use the appendices and what specific actions should I take to be prepared for next school year?

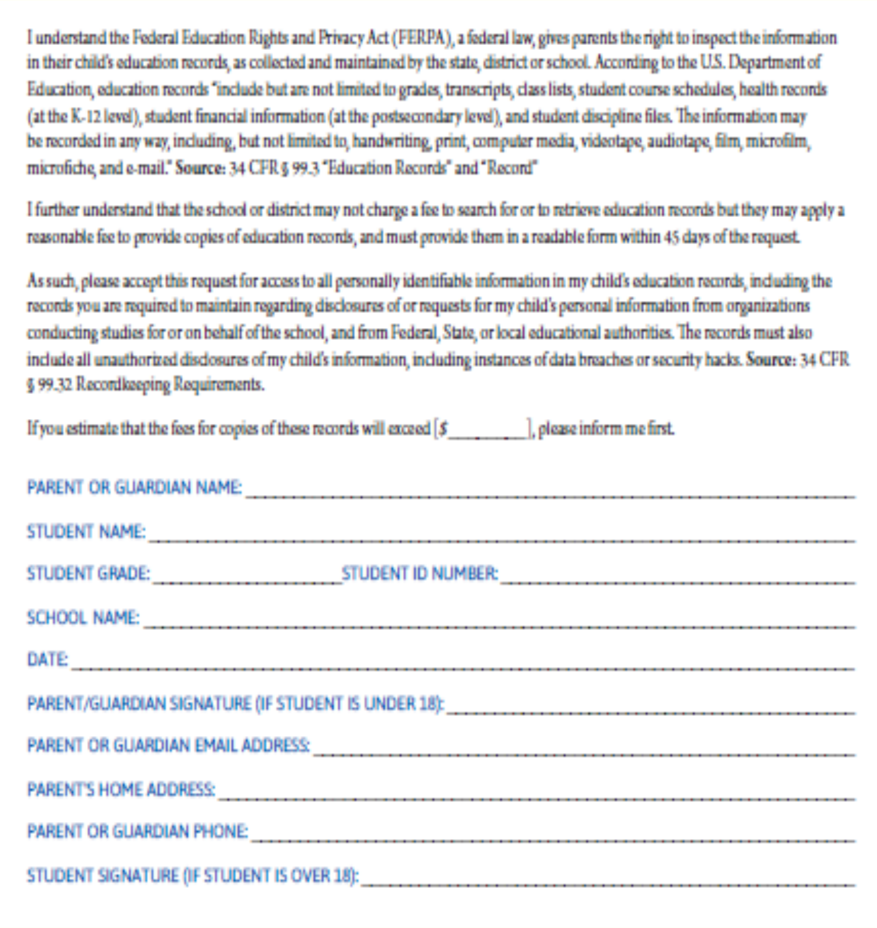
Parent Toolkit for Student Privacy: Appendix A

Request to inspect your child's education records held by the school, district, or state

- You have the right to inspect your child education records under FERPA
- Records must include any unauthorized disclosures from hacks or breaches
- If you disagree with anything in there, you can challenge it and have your view inserted into the records

How to use Appendix A:

Submit your form to your school or district. They have 45 days to respond.



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): ______________________

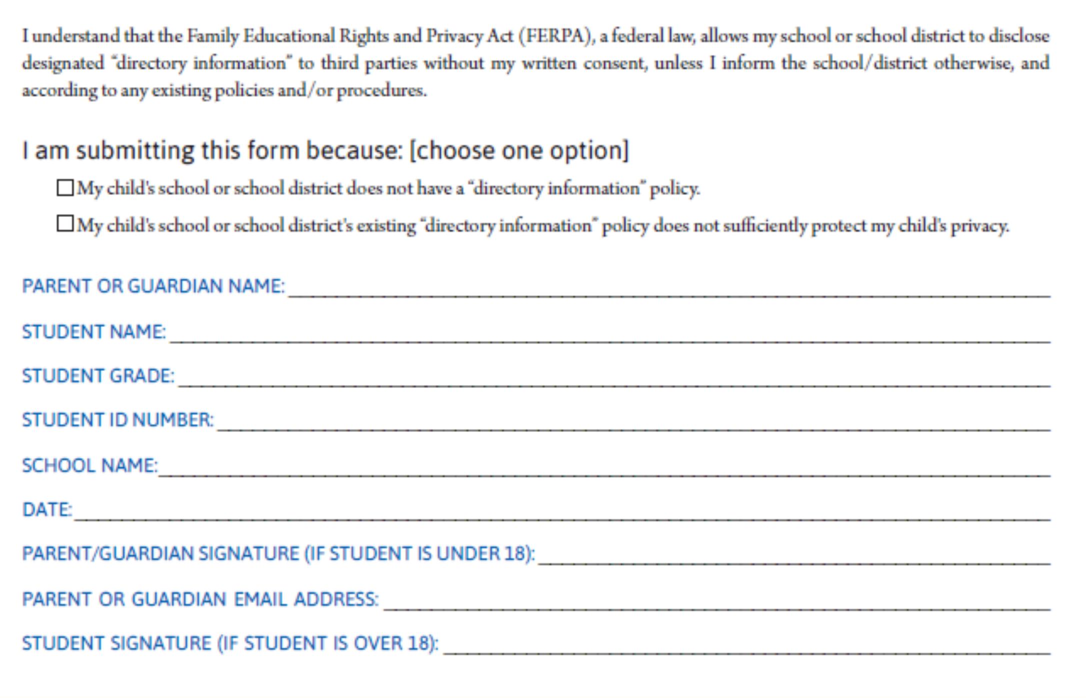
Parent Toolkit for Student Privacy: Appendix B

Sample letter to opt out of directory information

- Schools and districts can share "directory information" unless you opt-out
- Form puts you in control of what gets shared & with whom

How to use Appendix B:

Ask your principal for your school's form. If they don't have one, use ours! Be sure to get your form in at the beginning of school year.



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): ______

Parent Toolkit for Student Privacy: Appendix C

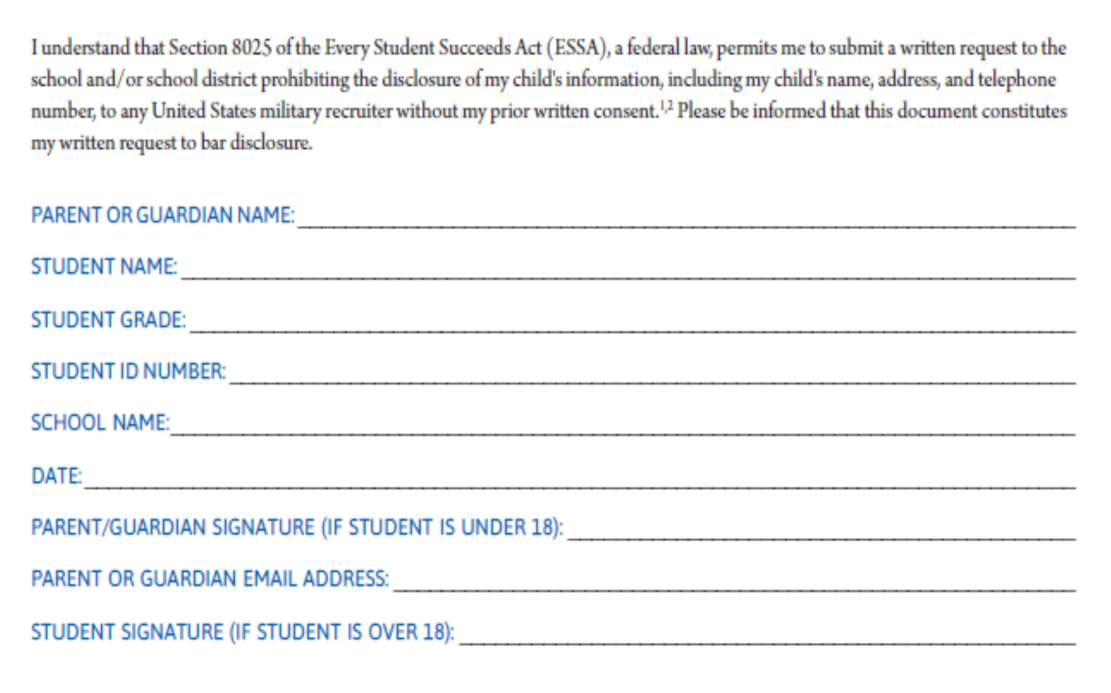
Sample letter to opt out of military recruitment

- For parents of high school students

- Prohibits school & district from disclosing information to any US military recruiter.

How to use Appendix C:

If your child isn't considering military service, use our form to opt-out.



I understand that Section 8025 of the Every Student Succeeds Act (ESSA), a federal law, permits me to submit a written request to the school and/or school district prohibiting the disclosure of my child's information, including my child's name, address, and telephone number, to any United States military recruiter without my prior written consent.[1,2] Please be informed that this document constitutes my written request to bar disclosure.

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): ____________________

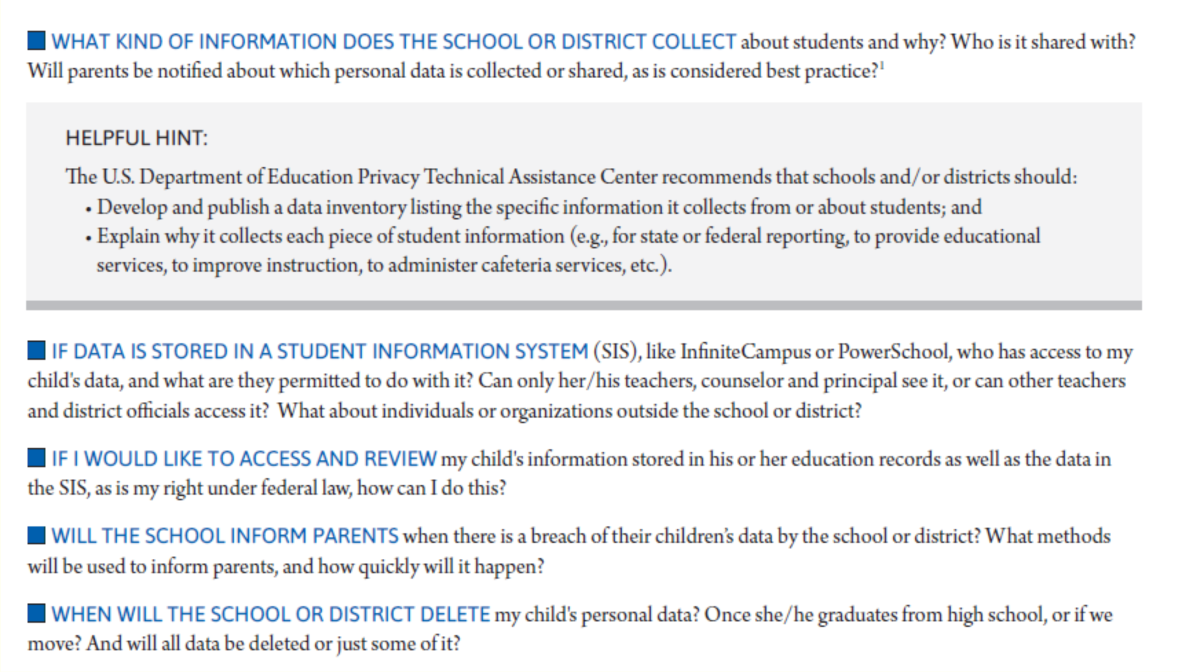
Parent Toolkit for Student Privacy: Appendix D

Additional questions to ask your teacher or principal

- Build on introductory questions in Section V.
- Organized by topics such as use of classroom apps, bring your own device, and online learning.

How to use Appendix D:

Decide which questions are most relevant/concerning to you. Keep a running list for when you meet with your teacher or principal.



■ 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?[1]

> 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?

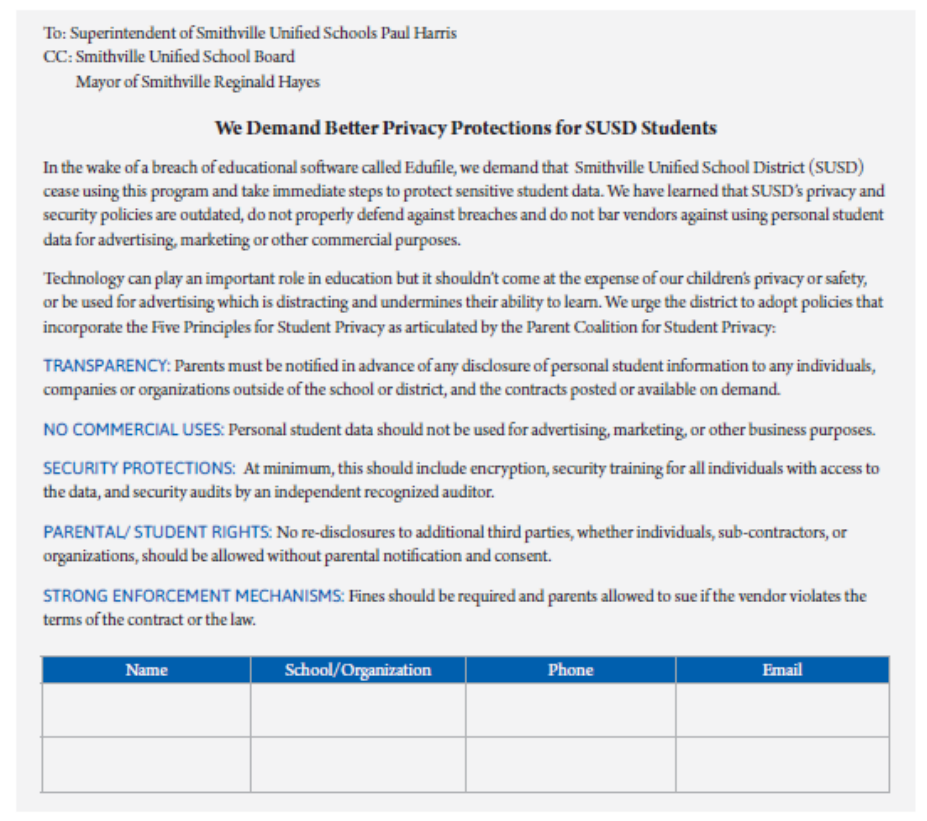
Parent Toolkit for Student Privacy: Appendix E

Sample petition

- Demonstrate the depth of concern in your community.
- Easy way to get other parents involved.

How to use Appendix E:

Be sure to update your petition signers on your progress and invite to any public meetings or events.



To: Superintendent of Smithville Unified Schools Paul Harris
CC: Smithville Unified School Board
Mayor of Smithville Reginald Hayes

We Demand Better Privacy Protections for SUSD Students

In the wake of a breach of educational software called Edufile, we demand that Smithville Unified School District (SUSD) cease using this program and take immediate steps to protect sensitive student data. We have learned that SUSD's privacy and security policies are outdated, do not properly defend against breaches and do not bar vendors against using personal student data for advertising, marketing or other commercial purposes.

Technology can play an important role in education but it shouldn't come at the expense of our children's privacy or safety, or be used for advertising which is distracting and undermines their ability to learn. We urge the district to adopt policies that incorporate the Five Principles for Student Privacy as articulated by the Parent Coalition for Student Privacy:

TRANSPARENCY: Parents must be notified in advance of any disclosure of personal student information to any individuals, companies or organizations outside of the school or district, and the contracts posted or available on demand.

NO COMMERCIAL USES: Personal student data should not be used for advertising, marketing, or other business purposes.

SECURITY PROTECTIONS: At minimum, this should include encryption, security training for all individuals with access to the data, and security audits by an independent recognized auditor.

PARENTAL/ STUDENT RIGHTS: No re-disclosures to additional third parties, whether individuals, sub-contractors, or organizations, should be allowed without parental notification and consent.

STRONG ENFORCEMENT MECHANISMS: Fines should be required and parents allowed to sue if the vendor violates the terms of the contract or the law.

Name	School/Organization	Phone	Email

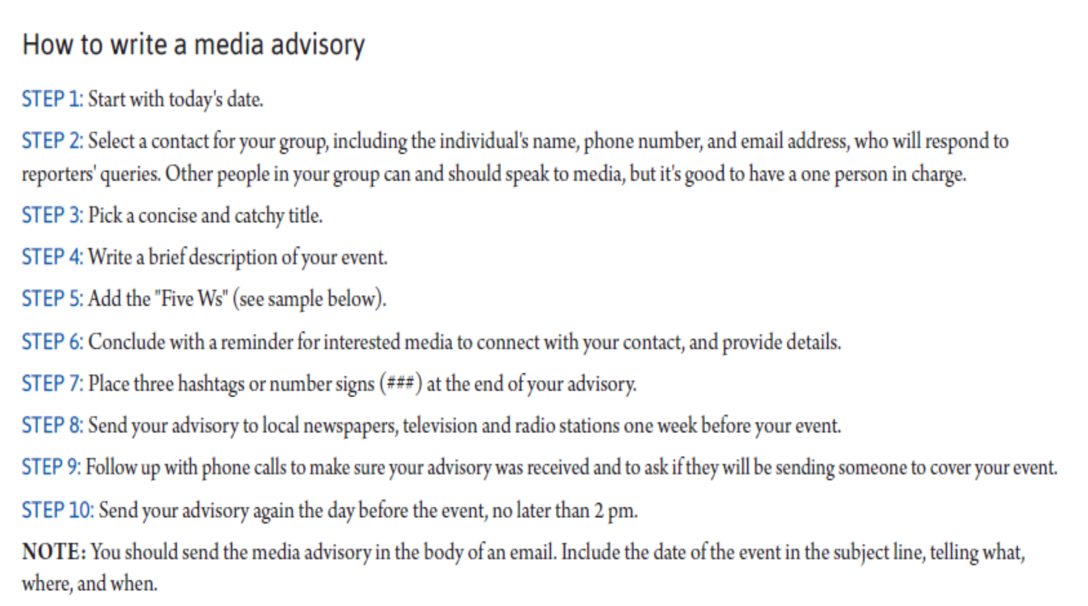
Parent Toolkit for Student Privacy: Appendix F

Tips for media outreach and press materials

- Media coverage is extremely useful for achieving your goals.
- Get to know your local reporters!

How to use Appendix F:

Use our sample media advisory and release as a template. Fill in with info about your event and quotes from members of your group



How to write a media advisory

STEP 1: Start with today's date.

STEP 2: Select a contact for your group, including the individual's name, phone number, and email address, who will respond to reporters' queries. Other people in your group can and should speak to media, but it's good to have a one person in charge.

STEP 3: Pick a concise and catchy title.

STEP 4: Write a brief description of your event.

STEP 5: Add the "Five Ws" (see sample below).

STEP 6: Conclude with a reminder for interested media to connect with your contact, and provide details.

STEP 7: Place three hashtags or number signs (###) at the end of your advisory.

STEP 8: Send your advisory to local newspapers, television and radio stations one week before your event.

STEP 9: Follow up with phone calls to make sure your advisory was received and to ask if they will be sending someone to cover your event.

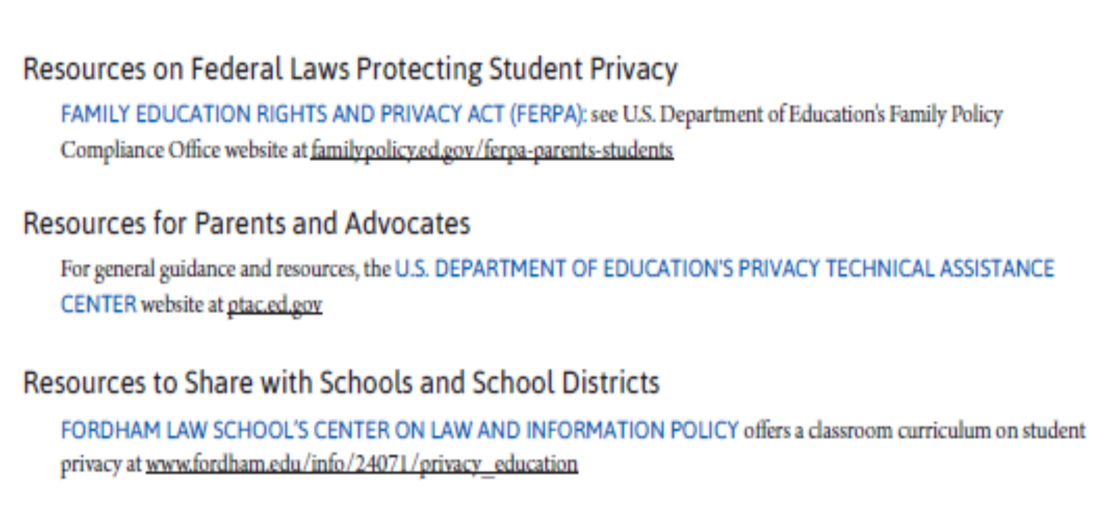
STEP 10: Send your advisory again the day before the event, no later than 2 pm.

NOTE: You should send the media advisory in the body of an email. Include the date of the event in the subject line, telling what, where, and when.

Parent Toolkit for Student Privacy: Additional Resources

Additional resources

- Topics range from "personalized learning"
- limiting children's screen time
- evaluating the privacy protections of specific apps and education software.



Resources on Federal Laws Protecting Student Privacy

FAMILY EDUCATION RIGHTS AND PRIVACY ACT (FERPA): see U.S. Department of Education's Family Policy Compliance Office website at familypolicy.ed.gov/ferpa-parents-students

Resources for Parents and Advocates

For general guidance and resources, the U.S. DEPARTMENT OF EDUCATION'S PRIVACY TECHNICAL ASSISTANCE CENTER website at ptac.ed.gov

Resources to Share with Schools and School Districts

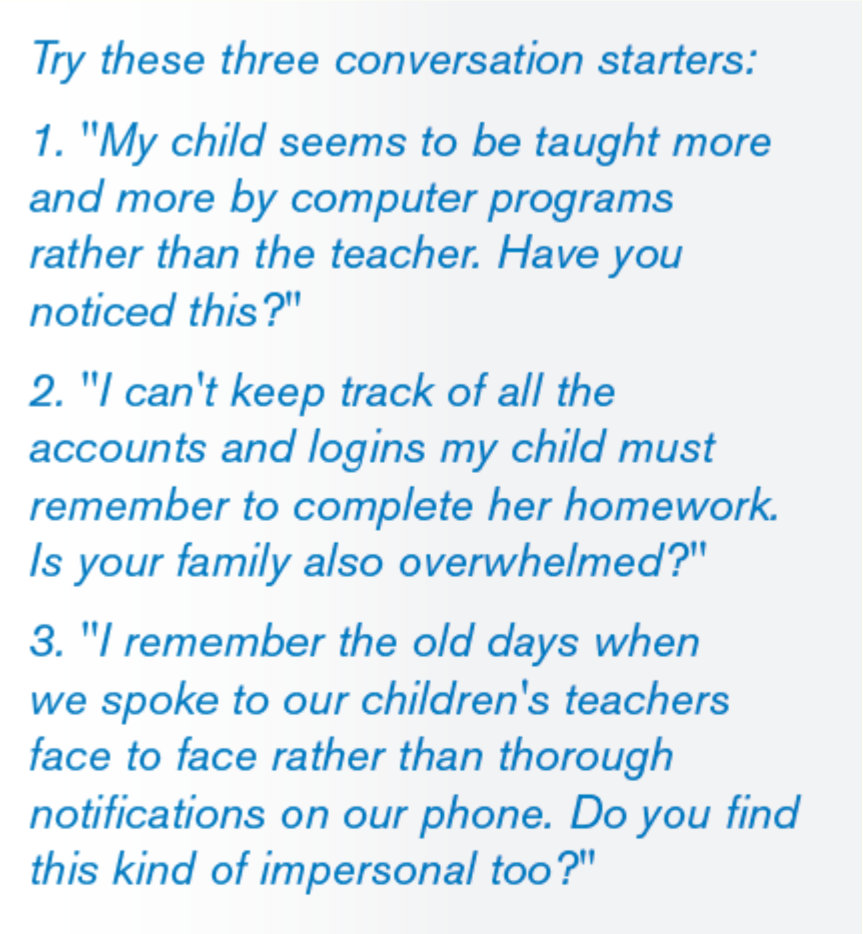
FORDHAM LAW SCHOOL'S CENTER ON LAW AND INFORMATION POLICY offers a classroom curriculum on student privacy at www.fordham.edu/info/24071/privacy_education

Tips for getting organized for next school year

- Get your forms in!
  - Opt out of military recruitment.
  - Opt out of disclosure of directory information. Remember: the deadline for opting out is often early in the school year.
  - Consider requesting your child's education record.
- Using Section V and Appendix D to make a list of questions you want to ask your principal or teacher.
- Make an appointment for early in the school year.

Tips for getting organized for next school year

- Talk to other parents and/or parent-teacher organization members
- Use media stories about student privacy or data breaches to start conversations.
- Start a group that shares articles, resources and concerns via email or social media.
- Share the Parent Toolkit for Student Privacy with other parents in your community!



Try these three conversation starters:

1. "My child seems to be taught more and more by computer programs rather than the teacher. Have you noticed this?"

2. "I can't keep track of all the accounts and logins my child must remember to complete her homework. Is your family also overwhelmed?"

3. "I remember the old days when we spoke to our children's teachers face to face rather than thorough notifications on our phone. Do you find this kind of impersonal too?"

Another concern: 2014 NY Student Privacy law not enforced

- A new student privacy law was passed by the NY Legislature in March 2014 - cancelling the inBloom contract.

- Law also called for NYSED to appoint a Chief Privacy & create Parent Bill of Privacy Rights that would include protections in state and federal privacy laws & be expanded via parent & public input

- Both supposed to be finalized by July 31, 2014; yet a permanent CPO, Temitope Akinyemi, wasn't hired until August 2016

- The current Parent Bill of Rights doesn't even include all the provisions of current state and federal privacy law, and has NOT been expanded through any public process

- We are urging NYSED to hold hearings on privacy and appoint a Stakeholder Data Advisory Board, as promised by 2009 in return for a $7.8M grant from US Department of Education

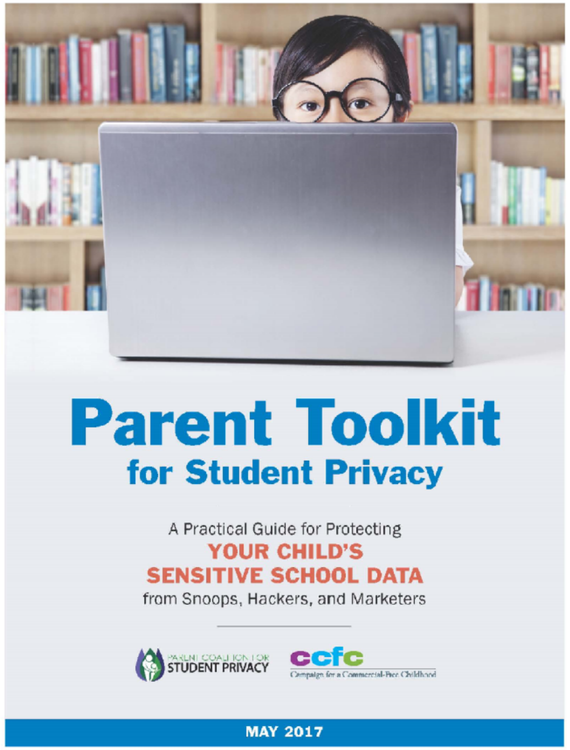
Questions?

Visit us at:

www.studentprivacymatters.org

www.commercialfreechildhood.org

Download your copy here:
HTTP://BIT.LY/PARENTTOOLKITSTUDENTPRIVACY



Parent Toolkit
for Student Privacy

A Practical Guide for Protecting
YOUR CHILD'S
SENSITIVE SCHOOL DATA
from Snoops, Hackers, and Marketers

PARENT COALITION FOR STUDENT PRIVACY

ccfc
Campaign for a Commercial-Free Childhood

MAY 2017