ExcelinEd

APRIL 2016

STUDENT DATA PRIVACY COMMUNICATIONS TOOLKIT

ABOUT EXCELINED

Founded by former Florida Governor Jeb Bush, the Foundation for Excellence in Education is igniting a movement of reform, state by state, to transform education for the 21st century economy by working with lawmakers, policymakers, educators and parents to advance education reform across America. Learn more at ExcelinEd.org.

EXCELINED.ORG

@EXCELINED

FACEBOOK.COM/EXCELINED

Table of Contents

Student Data Privacy Toolkit

Introduction

In recent years, student data privacy has emerged as a major issue in education and political arenas. Recent news coverage and social media conversations about student data access, especially as it relates to outside service providers, have heightened the public's overall interest in the security of student data. Meanwhile, many state legislatures have made moves to enact more state laws designed to protect the confidentiality of student education records. A significant communication challenge that school districts face is this conversation surrounding student data privacy.

In order to gain a more concrete understanding of what parents want to know about data privacy, ExcelinEd commissioned a representative survey of 800 individuals nationwide, 350 of which were parents of a K-12 student. Additionally, a focus group with K-12 parents was held in Tampa, Florida, to collect qualitative data. While student data privacy was not listed as a top concern when compared with other common education concerns, parents were much more likely to see it as an issue than non-parents.

One overarching message rose out of the findings: parents are looking to hear the clear boundaries that are in place to protect access and use of their child's data. Survey participants were more interested in what data was collected than how it would be used.

While participants view personalized learning as a positive for their children, personalized learning and the importance of student data in personalized learning instructional models were seen as separate issues from student data privacy. When talking data privacy, parents and participants wanted to hear about the laws, rules, and steps being taken to protect information about their children. And they want to hear the specifics:

- Who has access to student learning data?
- What data about my child do they have access to?
- How is the data being protected and kept secure?
- What laws are in place to protect student data privacy?

As the gatekeepers of student data, and parents' and guardians' primary point of contact as it relates to their child's education, school districts and schools should be prepared to both proactively and reactively respond to questions and concerns related to the privacy of student data. So how can districts communicate these details to parents? And, who is the best person to relay that message?

The first step to communicating with parents is to do so with honesty and transparency. Districts should reassure parents, with specifics, that they take student data protection seriously, but should also avoid speaking in absolutes or providing guarantees. If banks can get hacked, it is hard to believe that a school district cannot. Districts should communicate to parents exactly who has access to what data, including service providers. They should assure parents that they are in compliance with federal and state law, while also detailing the additional safeguards, training and plans they have put in place to protect student data.

Unlike most education topics where hearing from teachers and principals is preferred by parents, survey participants responded that they most want to hear from those with experience in data security and technology.

It is also important – through its communications and actions – that the district convey that protecting student data is an ongoing and continuous process, not a one-time project. Districts will need to maintain and update information about what data is collected, who is using it and what protections are in place to safeguard student data.

Purpose of this Toolkit

Parents expect school districts and schools to keep their children safe while they are in school. That expectation of safety and security also extends to the protection of their children's learning data. Therefore, it is critical that school districts and schools are open and transparent about their student data privacy practices, and that those efforts are clearly communicated to parents and other stakeholder groups. By sharing information on the types of student data collected, the purpose and benefits of collecting this information and the ways in which it is protected, school districts and schools can help dispel misperceptions about student data use and assuage concerns.

This student data privacy toolkit provides school districts and schools with recommendations on how to most effectively communicate with parents and other stakeholder groups about student data privacy, as well as a host of communications tools that can be used in these communications efforts. All toolkit resources are generalized for blanket use, so areas in which customized district-specific information are required are in brackets and highlighted in yellow. Districts also need to be sure that their policies, practices and procedures match the recommendations implied throughout the toolkit. Those instances will be noted as well.

Be sure to have appropriate school or school district personnel review and approve any communications or materials prior to releasing. This could include, but is not be limited to, the school or school district general counsel and privacy officer.

Additionally, while the focus of this toolkit is communicating data privacy practices and plans, demonstrating the value to data to parents is also important. When equipped with the right skills and tools, everyone who plays a role in education can have a strong impact on students and their communities. **Parents** can be their child's champion along the path to success. **Teachers** can be sure that their students are really learning what they are teaching. **Principals and district administrators** can use data to manage schools, allocate resources, and communicate with their communities. **Policymakers** can create the conditions for success in states and throughout the country. Education data are a powerful tool, but only if they are securely in the hands of the people who need the data, when they need the data. For more resources from Data Quality Campaign (DQC) and others to communicate the power of data to improve a child's education visit the Additional Resources section of this toolkit.

Target Audiences

Your target audiences are the groups of people with the most interest in your issue and with whom you expect to communicate. In relation to the issue of student data privacy and for the purposes of this toolkit, the primary target audience is parents and guardians. Most of the materials in this toolkit have been developed with parents and guardians in mind; however, there are materials that have been developed for secondary target audiences.

Primary Target Audiences:

- Parents and Guardians

Secondary Target Audiences:

- Teachers
- School and District Administrators
- School Board Members
- Local, State and Federal Elected Officials

Key Messages

Key messages are the main points you want to communicate to your target audiences. These messages should be the basis for and included in every communication you send or every presentation you make on a specific subject. On pages 12 - 14 of this toolkit, you will find student data privacy key messages broken down by target audience. When conveying information about student data privacy to each of the target audiences, it is important that these messages are consistently used and are part of any communication.

It should be noted that qualitative and quantitative research conducted as part of the development of this toolkit found that parents and guardians were most interested in knowing that school districts/schools were protecting student data and how they are safeguarding that information versus hearing about the benefits of student data.

When communicating with parents and guardians, it is recommended that school districts and schools lead with information on student data security and safety, emphasizing the priority the school district and school place on keeping students' learning data safe and secure.

Messengers

The student data privacy research also indicated that parents and guardians found local school board members, district and school administrators and independent, technology experts to be the most credible voices on the issue of student data privacy. To the degree possible, it is recommended that school districts and schools identify individuals who fall into these groups and gauge their willingness to serve as messengers on the issue of student data privacy. Messengers can be used for meetings and public presentations, media interviews and as authors of letters and newspaper opinion pieces.

Additionally, the research indicated that parents and guardians preferred not to receive information on student data privacy from their children's teachers. While teachers are often parents' and guardians' primary point of contact at their children's school, teachers were not viewed as student data subject matter experts and there was consensus among research respondents that the communication of student data privacy policies and practices should not be added to teachers' duties.

Proactive Communications

In addition to mandatory information on the Family Educational Rights and Privacy Act (FERPA) and Protection of Pupil Rights Amendment (PPRA), which school districts and schools are legally required to provide parents and guardians, school districts and schools should also proactively communicate the ways in which they protect all student learning data.

Communications aimed at parents should explain:

- The importance of protecting student data to school districts and schools
- How the school district and school protect student data
- The school district's/school's student data privacy policy
- That student data is restricted to authorized users
- That there are laws designed to protect student data with associated penalties for any misuse

The following recommended tactics will help school districts and schools openly, clearly and directly communicate with parents and guardians about student data and what steps schools districts and schools are taking to keep this information safe.

Proactive Tactics

Student Data Privacy Policy – Prior to the beginning of the school year, post a copy of the school district's or school's Student Data Privacy Policy to the district's or school's website.

Student Data Web Page(s) – Dedicate a page or pages on the school district or school website to student data privacy information. In addition to the Student Data Privacy Policy, and other resources we recommend posting include:

- Student Data Privacy Fact Sheet ("Eight Things to Know About Student Data"; page 19),
- Student Data Privacy Frequently Asked Questions document (pages 16 – 18), and
- Student Data Privacy Infographic (page 35).

Template verbiage for this web page(s) can be found on page 15. Ideally, this web page or pages would be completed before the start of the school year.

Student Data Web Banners – Utilize student data and student data privacy web banners to direct web visitors to the dedicated student data privacy web page(s). The banners could be housed on the home pages or "families/parents" pages (if applicable) of the school district's and school's websites. The banners would then hyperlink to the dedicated student data privacy web page(s). A variety of banner designs and sizes have been included in this toolkit (page 36).

Letter to Parents/Guardians – Include a brief letter to parents and guardians regarding your school/school district's student data privacy policies and practices in the "welcome back/back-to-school" parent guides and packets, as well as new student orientation packets. A template letter can be found on page 20, which provides general information about the types of data collected, why it is collected and how it is protected. School districts and schools should update the template with their school district and school information and personalize it to their school district/school community. Letter text that directs parents and guardians to the Student Data Web Page(s) should be removed if a dedicated Student Data Web Page is not created.

Talking Points – Talking points help provide basic information on a subject and serve as a way to keep people on track when discussing a particular issue. This toolkit provides talking points for a number of different education stakeholder groups to use as needed when discussing student data privacy. The talking points on pages 21 – 25 are broken down by target audience/stakeholder group.

Proactive Communications Timeline

Prior to the start of the school year

- Work with appropriate school and district staff to develop a Student Data Privacy Policy

- Post the Student Data Privacy Policy on the school district or school website

- Create a dedicated Student Data Privacy Web Page or Pages on the school district or school website; utilize the template web page verbiage, Student Data Privacy Fact Sheet (“Eight Things to Know About Student Data”), Student Data Privacy Frequently Asked Questions document and Student Data Privacy Infographic for content

- Post student data web banners on the school district’s and/or school’s home pages or “families/parents” pages (if applicable); hyperlink the banners to the Student Data Privacy Web Page(s)

At the beginning of the school year

- Distribute the parent/guardian letter via “welcome back/back-to-school” packets sent to parents and guardians and through new student orientation packets

As needed

- Brief stakeholders, including school board members, PTA leaders and state lawmakers, on your current student data privacy policy and, as applicable, the steps being taken to improve the safety and security of student data information and records

- Provide student data privacy talking points to target audiences/education stakeholder groups as needed

Rapid Response Communications

While parents and guardians who took part in the toolkit development research indicated a general interest in communications that explained student data security measures, the majority did not wish to be inundated with information on the subject of student data. However, fresh news coverage and social media conversations on the issue may lead to heightened interest among parents, guardians and other stakeholder groups.

Should concerns about student data privacy grow among these stakeholder groups and the school district and/or school starts to receive an increasing number of questions on the issue, the school district and schools must be prepared to respond.

The final portion of the toolkit outlines a rapid response plan that can be implemented only if needed. The following rapid response communications tactics will help school districts and schools answer questions, assuage concerns and dispel misinformation about student data and student data privacy.

Rapid Response Tactics

Newsletter Article/Email – Send an email to the school district or school parent and guardian listserv regarding the school district's and school's strict student data protection measures and direct them to the Student Data Privacy Web Page(s) for more information. Include a contact name and phone number and/or email address in case parents and guardians have additional questions. This same information could also be included in a monthly school newsletter. A template newsletter article/email communique is included on page 26. This information should be sent or posted as soon as questions and concerns arise.

Fact Sheet – Consider sending parents and guardians a hard copy of the Student Data Privacy Fact Sheet ("Eight Things to Know About Student Data") that is posted on the Student Data Privacy Web Page(s). The fact sheet on page 19 can be sent home with students or sent via postal mail.

Social Media – When interest in student data privacy is elevated, share information through social media posts on a weekly basis until the frequency of questions and parent/guardian concerns has lessened. Template social media posts can be found on pages 32 – 34 and can be reused over the course of several weeks or months. To the degree possible, use graphics and images to help visually communicate key messages on student data privacy. Graphics that can be used for social media and other purposes are located on page 37.

Lawmaker Brief – Parent, guardians and other stakeholder groups may look to local, state and federal elected officials for answers on student data privacy and to demand action. It is critical that elected officials have accurate information on the issue so they can communicate the facts to their constituents and help school districts/schools correct misconceptions. If school districts and schools begin to experience an increase in student data privacy questions, school district administrators should conduct outreach to lawmakers at all levels to share background information and talking points on the issue. A template lawmaker brief, which provides an overview of the issue, details on federal laws related to student privacy and key points, can be found on pages 27 – 28. This is a good "leave behind" to provide lawmakers. Copies of talking points specifically developed for elected officials (pages 24 – 25) should also be provided. The Data Quality Campaign has an excellent infographic that outlines *What is Student Data* that could be provided, as well.

News Media Outreach – Increased news coverage of student data privacy may be the genesis for rising parent and guardian concerns, or could be a natural byproduct of increased interest among education stakeholder groups. With so many people relying on news outlets for their information, it is important that news coverage of the issue is accurate. As stakeholder interest and media inquiries increase, the school district Public Information Office should conduct outreach to local broadcast, print and digital news outlets and share information on the measures in place to protect student data. Tools such as the Student Data Privacy Fact Sheet ("Eight Things to Know About Student Data"; page 19), Student Data Privacy Frequently Asked Questions document (pages 16 – 18), and Student Data Privacy Infographic (page 35) could all be shared with members of the press.

Newspaper Opinion Pieces – To ensure the school district's messages on student data privacy and security are communicated in area newspapers, the school district should consider submitting an opinion piece to local daily and weekly newspapers. There are typically two types of opinion pieces that newspapers will run – a shorter, letter to the editor (usually between 200 and 300 words) and a longer piece known as an opinion-editorial or op-ed (words limits vary from newspaper to newspaper, but generally range from 400 to 800 words). One of the major benefits of a letter to the editor or op-ed is that the author can convey key messages in an unfiltered format. Letters to the editor and op-eds are generally submitted to the newspaper's editorial board editor. This toolkit includes two sample letters to the editor and one template op-ed (pages 29 – 31). Based on the toolkit development research, it is recommended that a district administrator, such as the district superintendent, or a local school board member serve as the author of the op-ed.

In addition to district administrators and local school board members, the research indicated that independent technology experts were also considered trusted sources on this subject. If your school has a relationship with an independent technology expert who has or will review your policy and practices, ask him or her to submit a letter or op-ed to the local newspaper editor based on the template language provided.

Talking Points – Distribute the talking points on pages 21 – 25 to each target audience/stakeholder group that could potentially serve as a messenger on the issue of student data privacy. The talking points will provide each group with a framework to respond to questions and generally address the issue of student data privacy. The talking points should be reviewed with each group and an opportunity to answer their questions provided if possible.

Crisis Communications Planning

While not as likely a target as financial or other highly sensitive data, a breach involving student data could occur and school districts and schools should be prepared for such an event in case it happens. Should the district or a school become aware that student data has been misused or compromised, it is critical that parents and other stakeholders look to the district or school for accurate, timely information on the situation rather than third parties, including the media, who may not have a complete or accurate picture. A thoughtful, crisis communications plan developed in advance of a crisis can help mitigate the damage, quickly correct misinformation and restore confidence. Here are a few tips to help prepare a crisis communications plan around a student data breach scenario:

- Assess the organization's strengths and weaknesses as it relates to student data security and run through various scenarios where student data could be misused or compromised.

- Determine how the school district or school should react to those different scenarios.

- Establish a crisis communications team by identifying all staff members who will play a role in gathering and communicating information about the student data breach.

- Provide ongoing crisis communications training to this team and run through these potential student data breach scenarios with your crisis communications team on a regular basis.

- Designate a media spokesperson or spokespeople who will be the only ones to provide comment to the media regarding the evolving situation.

- Communicate with parents and other stakeholder groups as soon as possible following an incident, but be sure you have as many verifiable facts as available before you start communicating.

- Once you're ready to communicate, share basic information about what occurred, what steps the district/school is taking to remedy the situation and the policies/procedures being put into place to help prevent this from occurring again.

Toolkit Resources – Written Materials

Student Data Privacy Key Messages

Key Messages to Give to Parents

- Student data is carefully safeguarded through school and district policies and procedures, as well as federal and state privacy laws that are specifically designed to protect student data.

- Individuals within the district only have access to the identifiable data they need in order to carry out the responsibilities of their job.

- We collect data including scores on tests and assignments, report card grades, attendance, demographics, information on special needs, graduation and remediation rates, and disciplinary actions. This data is used to determine eligibility for services and to personalize lesson plans for learning and thereby improve student achievement.

- Our schools, school districts, and technology partners are subject to strict penalties under law if student information is misused or compromised.

- Information collected about your child’s learning helps our teachers and schools enhance his/her educational experience to ensure student success.

Key Messages from Teachers

- Our access to personally identifiable data about student learning is limited to those students with whom we work.

- As teachers, we are trained and committed to protect the student data we can access.

- Student data allows us to personalize lesson plans and assignments and select the right learning tools and content for each student.

Student Data Privacy Key Messages - Continued

Key Messages from School & District Administrators

- Our district recognizes that the security of student data is of the utmost importance and we serve as the frontline in the protection of student data.
- Our school/district has a comprehensive student data privacy policy that outlines processes and security mechanisms that protect student data and also governs who has access to data and how it can be used.
- Access to personally identifiable information is restricted to trained, qualified people. And they only have access to the specific data they need to do their jobs.
- Student data helps principals and school district administrators make important decisions on how to best serve our students. We limit the data we collect to only that which is necessary for us to provide students with an effective education.

Key Messages from Local School Board Members

- As leaders elected to oversee our community’s school system, we are committed to protecting and securing student data.
- It is our duty to ensure the school district and its employees are upholding all existing federal and state student privacy protection laws and we take that responsibility very seriously.
- Aggregated student data allows our board to make informed decisions on the allocation of resources and establishment of new programs that will enhance students’ learning.

Student Data Privacy Key Messages - Continued

Key Messages from Elected Officials

- As elected officials, it is important for us to know how well the students and schools in our community/state/nation are performing academically.

- The information we receive is aggregated data about attendance, graduation rates, and test scores – not data that is personally identifiable. This data allows us to make informed decisions about the establishment of new programs and allocation of resources that will enhance student learning.

- It is equally important that personally identifiable data is protected and used only for its appropriate purposes.

- As elected officials, it is our duty to raise awareness as to what data the state collects and communicate why they are collected in a clear and transparent manner to all stakeholders.

- We/I will remain in contact with the schools/school system in my district/community to ensure they have the proper policies and procedures in place to protect student data.

Student Data Privacy Web Page Content

Protecting Your Child’s Data

Schools and school districts have always collected data on students. Instead of paper files, much of that data is now collected through computers and online resources. While the systems for organizing and managing this information have changed over the years, our school’s/school district’s commitment to confidentiality remains the same.

It is our responsibility to ensure the security of each student’s education record and we take that responsibility very seriously. There are also existing federal and state laws in place that protect student information. Our school/district has a comprehensive student data privacy policy that outlines security mechanisms that protect student data.

A copy of our school district’s student data privacy policy can be viewed below. Please take a moment to review it and the other student data privacy resources available.

Our Privacy Policy [insert hyperlink]

Fact Sheet – Top Eight Things to Know About Student Data [insert hyperlink]

Frequently Asked Questions About Student Data Privacy [insert hyperlink]

Student Data Infographic [insert hyperlink]

Student Data Privacy Frequently Asked Questions

STUDENT DATA PRIVACY

Frequently Asked Questions

What kind of data is collected about students?

Our district collects demographic information (names, parents' or guardians' names, address, gender, date of birth, etc.), as well as information such as test scores, copies of assignments and homework, report card grades, student attendance, eligibility information for free or reduced price lunch and other programs, information about special needs and services, graduation and remediation rates, and disciplinary actions. Some additional data about students we may collect includes student use of school provided software, networks and technology devices, as well as the use of school provided communications services such as email.

What kind of information is collected about parents?

We collect name, address, and contact information from parents and may also collect income information to verify eligibility for programs such as free and reduced price lunch. We may also store information about your communications with district staff (e.g. in a teacher's or administrator's email archive). Our district **does not** collect or store sensitive information, such as parents' or guardians' social security numbers, driver's license numbers, political views and religious affiliations.

How is student data used?

Administrative	**Student registration, Course scheduling, Guidance counseling, Attendance, School lunch programs, Busing services**
Instructional	Homework assignments, Instructional tools and learning apps, Working collaboratively online, Engaging with teachers and classmates, Tailored course curricula, and Support services
Assessment and Measurement	Measuring the quality of education, Standardized tests, Course assessments, Reshaping classroom materials, Measuring effectiveness of student learning
Optional and Non-Educational	School yearbooks, Class photos, PTA fundraising, School paraphernalia

What is the difference between personally identifiable data, de-identified and aggregate data?

- Personally identifiable information refers to any information that could identify your child. This includes, but is not limited to: their name, parent or family members' names, address of student or family, birth date, email address, telephone number, social security number, geolocation information, screen names, user names, photographs, and videos.
- De-identified data refers to the process of anonymizing, removing or obscuring any personally identifiable information from student data to prevent the unintended disclosure of the identity of the student and information about him/her.
- Aggregated data is summarized information about a group of students and does not include any identifiable information on individual students.

Who has access to data about my child?

Our district has developed policies that limit access to personally identifiable data based on an individual's role within the district and what is referred to as their "legitimate educational interest" in information about a student. For instance, a bus driver needs to know a child's address and possibly limited health information in order to get students home safely, but access to information about student test scores is not needed for the bus driver to properly carry out his or her job.

Teachers, principals and other administrators will have access to the widest range of information about your child in order to monitor their progress in school. Outside service providers to the school receive only the information about your child needed to provide particular services. This could mean letting a tutor know what a child needs help on or providing a student's name to a math software company so the child can log in and their teacher can monitor their progress.

School board members, the state department of education and the U.S. Department of Education receive aggregated information that allows them to understand how our schools are performing and make decisions about programs and resources. Personally identifiable information may be shared in limited situations such as to review appeals of school decisions or to audit and monitor programs.

Who is responsible for protecting student data?

Our schools and district officials closely safeguard education records and the personally identifiable information that make up those records. Access to this data is restricted to trained, qualified individuals who only have access to the specific data they need in order to do their jobs. Our district has a comprehensive student data privacy policy that all staff, faculty and service providers are required to follow. This policy outlines security mechanisms that protect student data and also governs who has access to data and how it can be used.

What kind of security measures are used?

In order to ensure that our students' data is properly protected, our district has contracted with independent information security experts to review our policies and practices to protect student data. We have also deployed strategies to protect our information systems such as encryption, firewalls, intrusion detection software, activity logs and regular training of staff with access to sensitive information.

Are there existing laws that protect student data?

Yes, there are multiple federal and state laws that are designed to protect student data and prohibit any misuse. If student information is misused or compromised, school districts, including our own, can be subject to strict penalties.

How do schools hold outside service providers accountable for maintaining the confidentiality of the student data they receive?

Our school district is responsible for holding outside service providers accountable and ensuring they have the appropriate protections in place to safeguard the student data they receive. Our contracts with service providers include protections. And, just like any member of the school/school district staff or faculty, outside service providers are expected to adhere to our student data privacy policy. Companies working with schools and the district are only permitted to use student information for its authorized purpose. Any misuse of the data would constitute a breach of contract and may also violate state and federal laws, which may result in penalties.

Who owns student data?

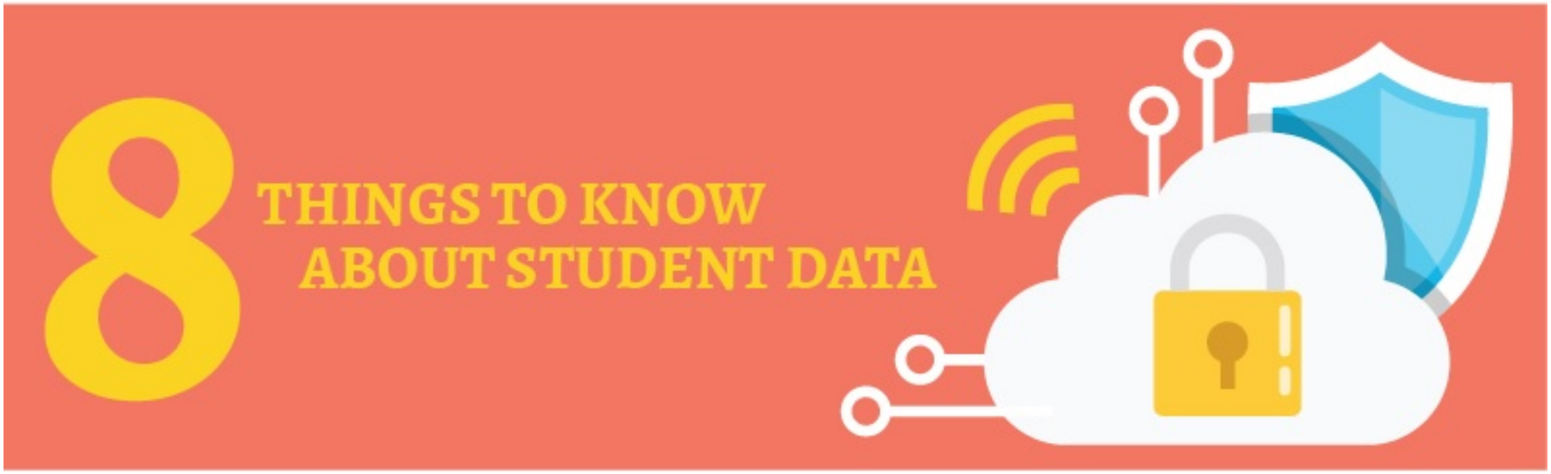
Our schools and school district retain ownership of student data and are the stewards of this data.

Can parents access their child's education records?

Yes. Under federal law, parents have the right to review their child's education records. Please contact *[insert name of contact]* to request access to and a copy of your child's record.

If you wish to learn more about the software and tools used in your child's classroom, please contact their teacher who will provide access to a parent account or share relevant reports about your child's use of these tools with you.

Student Data Privacy Fact Sheet



1. We take our responsibility seriously to keep information about your child safe and secure.

2. Strict privacy and security policies established by the school district, as well as state and federal student data privacy laws, protect your child's data. These laws limit what kinds of data can be collected and restrict sharing of that data. You can read our Student Data Privacy Policy on our district's website: *[insert website url]*

3. There are punishments and penalties in place for misusing student data or breaking these laws and policies.

4. Access to data in our district is restricted to authorized users only. Users, including service providers to the district, are only given access to the data they need to do their jobs.

5. Our teachers are trained and committed to protect your child's data.

6. Student data allows our teachers to personalize learning for your child and helps ensure he/she succeeds in school and beyond.

7. Data helps provides an accurate and up-to-date view of how our schools, teachers and students are performing.

8. You can ask for your child's education record at any time. Contact us at *[insert name at XXX-XXX-XXXX or insert email address].*

Student Data Privacy Letter to Parents/Guardians

Dear Parents and Guardians,

We wanted to make sure you were aware of the ways in which we are protecting data collected about your child and how it is used to enhance his or her learning experience. Please know that we are committed to protecting your child's education records. Our school district has developed comprehensive policies to comply with federal and state student privacy laws and regulations and is subject to strict penalties if student information is misused or compromised.

Our district and schools collect data including scores on tests and assignments, report card grades, student attendance, demographics, information on special needs, graduation and remediation rates, and disciplinary actions. This data is used to determine eligibility for services, help teachers and school leaders understand what is or is not helping children succeed, and to personalize instruction to improve student achievement. While schools and school districts have always collected student data, the creation, storage and analysis of this information has increasingly moved to digital formats online.

As a result, we have a strict student data privacy policy in place that details the procedures and security mechanisms in place to protect student data. The policy also outlines restrictions on authorized users who are permitted to access student data. Access to personally identifiable data about your child is limited to those with a legitimate educational interest in their data, meaning that individuals within the district only have access to the data they need in order to do their job.

A copy of our student data privacy policy can be found on the [insert district name] website at [insert url]. This data will never be sold or shared for marketing or commercial purposes, and will only be used to improve how our students learn and succeed.

If you have any questions or concerns, you may visit [insert url] or contact [insert name] at [insert email/phone number].

Thank you and we look forward to a successful school year.

Kind Regards,

[insert signature]

Student Data Privacy Talking Points

Talking Points to Use When Communicating with Parents

Data Collected

- Our schools and districts collect data including scores on tests and assignments, report card grades, student attendance, demographics, information on special needs, graduation and remediation rates, and disciplinary actions. This data is used to determine eligibility for services and to personalize lesson plans for learning and thereby improve student achievement. We also collect information about the use of the school's network, as well as school provided software and computing devices.
- We collect name, address, and contact information from parents and may also collect income information to verify eligibility for programs such as free and reduced price lunch. We may also store information about your communications with district staff.
- Our district does not collect or store sensitive information, such as parents' or guardians' social security numbers, driver's license numbers, political views and religious affiliations.

Protections

- Maintaining the confidentiality and security of your child's education records is critically important to our school/school district.
- Our district and schools have collected and protected information – such as course enrollments, grades and test scores – about students for decades. As this information has moved online and schools have deployed new technologies to help students learn, we have developed new policies and procedures to protect your child's data in this digital age.
- The school/school district has a comprehensive student data privacy policy that outlines the processes, procedures and security mechanisms in place to protect student data.
- This policy also governs who has access to data and how it can be used.
- We restrict data access to qualified, authorized users as a safeguard to ensure that student data is secure.
- Our district complies with multiple federal and state privacy laws in place to protect student data.

Student Data Privacy Talking Points - Continued

- Our district and schools are subject to strict penalties if student information is misused or compromised.

How Data is Used

- Data provides teachers valuable information about your child’s progress – where he/she is doing well and where he/she might need some extra help or instruction.
- Analyzing this kind of information allows teachers and schools to tailor and personalize learning just for your child.
- Our district also uses aggregated data about groups of students to make decisions about the curriculum, assessments and supports we use across classrooms and schools.

Talking Points for Teachers to Use If Asked By Parents about Student Data Privacy

- As teachers, we are trained to protect the student data we can access.
- Our district has a clear student data privacy policy which you can review on the district’s website.
- We collect and use data such as records of assignments and homework, test and quiz scores, report card grades and attendance.
- We can also track student progress through programs and apps students use in our classes. The software we use has been reviewed to ensure it complies with our privacy policy.
- Data allows us to see where students are doing well and where they might need some extra help. It helps us personalize lessons and assignments to what each student needs.
- Student learning data provides us with information that allows us to teach more effectively, which in turn helps students learn more effectively.
- If you would like more information about student data privacy, I encourage you to visit the school/school district website and talk with administrators in the front/district office.

Student Data Privacy Talking Points - Continued

Talking Points for School & District Administrators to Use When Communicating with Parents or Other Key Stakeholders about Student Data Privacy

Protections

- As the frontline protectors of student information, our responsibility to safeguard student data and keep it secure is of the utmost importance to our school/school district.

- Our school/district has a comprehensive student data privacy policy that outlines who has access to data, how it can be used and security mechanisms in place to protect student data.

- Access to student data is restricted to qualified, authorized users only.

- Teachers, other staff members and service providers are only given access to the specific pieces of data they need to do their jobs and not a student's complete record.

- Our contracts with service providers who access student data in order to perform their specific function include strict controls to protect student data.

- We maintain control over any personally identifiable information.

- We comply with all existing federal and state student data privacy laws and ensure our staff, faculty and service providers do the same.

How Data is Used

- Everything we do is focused on the ultimate goal – making sure our students are well prepared to succeed in college, their careers and life – and student data provides important information to help us achieve that goal for your child.

- Data helps principals and school district administrators make important decisions on how to best serve each student.

- Not only can we look at the performance of individual students and teachers, we can get a sense for how well students and schools are performing on a school-wide/district-wide basis.

Student Data Privacy Talking Points - Continued

- This helps us figure out how to best apply our resources and provide services, including administering different programs, such as transportation, assistance programs and programs for students with special needs.

Talking Points for Local School Board Members to Use When Communicating with Parents or Other Key Stakeholders about Student Data Privacy

- Our community counts on us as school board members to make smart choices for our students.

- As the leaders elected to oversee our community's school system, we are committed to the security and privacy of student information.

- Our district has developed a comprehensive student data privacy policy that outlines security mechanisms that protect student data and also governs who has access to data and how it can be used.

- It is our duty to ensure the school district and its employees are adhering to this policy and are upholding all existing federal and state student privacy protection laws.

- We take that duty very seriously and have faith that our district and school administrators, faculty and staff share our commitment to protecting our students' education information.

- Being able to analyze and review data on the students and schools in our district allows us to make informed decisions on everything from the implementation of policy to the allocation of resources to the establishment of new programs.

- Most importantly, it enables us to see which educational programs are effective and are increasing student achievement.

Talking Points for Elected Officials to Use When Communicating with Parents or Other Key Stakeholders about Student Data Privacy

- As elected officials, we understand the value in having the kinds of information you need to create sound policy.

- State and local education systems have used student data to inform decisions and make important strides in student achievement in recent years.

Student Data Privacy Talking Points - Continued

- Data helps leaders see what’s working and what’s not and make informed decisions going forward.

- As a representative of the people in my community/district/state, it is important for me to have aggregated data on how well the students and schools in my community/district/state are performing.

- Many times this information is used to make federal and state education funding decisions.

- It is equally important that any personally identifiable data schools control is secured, kept confidential and used for appropriate purposes.

- We/I will remain in contact with the schools/school system(s) in my district/community/state to ensure they have the proper policies and procedures in place to protect student data and that those policies and procedures are in line with federal and state laws.

Rapid Response Tool: Student Data Privacy Newsletter Article/Email

You may have heard some things in the news or social media about student data privacy. So, what exactly is student data and how is it used? Basically, it's the information schools and schools districts collect on your child throughout their education career, including scores on tests and assignments, report card grades, attendance, demographics, information on special needs, graduation and remediation rates, and disciplinary actions. This data is used to determine your child's eligibility for services and to personalize your child's learning experience to help him/her be as successful as possible in school.

Schools have always collected this information on paper, but nowadays that information has moved to electronic and online formats. Today's technology has also given educators the opportunity to use online resources for instruction and evaluation. Whether in a folder in a filing cabinet or an electronic file stored in a computer, [insert school/school district name] takes the privacy of your student's data very seriously.

We have a strict student data privacy policy, which you can view at [insert url]. Access to student data is restricted to authorized users and there are security mechanisms and protocols in place to keep your child's education record confidential. The student data privacy page on our website includes a copy of our policy, as well as other helpful information, such as fact sheets and frequently asked questions. We encourage you to check this information out.

If you have any questions or concerns, please visit [insert url] or contact [insert name and contact information].

Student Data Privacy Lawmaker Brief

STUDENT DATA PRIVACY – LAWMAKER POLICY BRIEF

Addressing Constituent Concerns Over Student Data Privacy

Issue

Collecting and analyzing information about student learning is vital to helping our students succeed. While student data has been collected for decades, new technology has shifted more of this data collection online in digital formats. As we move into an increasingly digital age, questions from the public, and parents in particular, have arisen about how student data is collected, used and protected. A primary concern is access to student data – who has access, what types of data can they access and whether or not this data can be used for marketing or commercial purposes. Recent news coverage and social media conversations about student data access, especially as it relates to outside service providers, have heightened the public's overall interest in the confidentiality and security of student data. As a result, policymakers and lawmakers should be prepared to respond to constituent questions and concerns regarding the privacy of student learning data.

Facts

Our district has a comprehensive student data privacy policy that governs who has access to data and the types of data they can access. Access is restricted, and we have layers of security measures to help keep students' education records confidential. Our contracts with technology partners include strict controls and clear requirements to protect student data. These providers are only given access to the data they need to do their jobs. Additionally, there are federal and state laws designed to protect student data privacy. Misuse of this data will result in severe penalties.

Federal Laws Protecting Student Data

Family Educational Rights and Privacy Act (FERPA) – guarantees that parents have the right to review and make changes to their children's education records. FERPA also restricts who can use and access student information.

Children's Online Privacy Protection Act (COPPA) – controls what information is collected from children under the age of 13 by companies operating websites, games and mobile apps.

Protection of Pupil Rights Amendment (PPRA) – outlines the type of information that can be asked of students in federally-funded surveys or evaluations. Under PPRA, parents have the right to view these surveys and evaluations, require parental consent for response to surveys and evaluations related to sensitive subjects and to opt out of certain types of marketing materials.

State Laws Protecting Student Data

[insert information on data privacy legislation and laws in your state]

Policy Implications

Our district has made important strides in student achievement in recent years. This is partially due to our ability to use student data to inform the decisions of teachers, principals, the superintendent and school board members. Analysis of student data allows us to identify students' needs, provide access to innovative tools and technologies, determine what programs work and reward our most effective teachers and principals.

As legislation and policies are considered to protect student data, it is critical that these efforts do not produce unintended consequences that would limit these safe and effective uses of data. We know it is critically important to protect students' data, but that needs to be done in ways that will allow our teachers, principals and administrators to continue to drive innovation and results for our students. State and local education systems have been able to make important strides in student achievement in recent years because they have been able to gather, analyze and review a wide spectrum of student data. As the federal government and states consider legislation and policies designed to further protect student data, it is critical that these efforts not inadvertently limit the safe and effective use of data. Without access to secure, authorized data, the progress made by schools across the country could be hindered or even reversed.

Key Points

- Protecting student data is a high priority in our school district.
- Our district has strict policies and procedures in place to protect student data.
- There are state and federal laws regulating what data can be collected about students, and how and who can use that data. There are severe penalties for misuses of such data.
- Schools are limited in the types of information they can collect and how to use it.
- It is important to use student data to understand how well students in our community, state and nation are performing.
- Data has enhanced schools' and teachers' abilities to tailor instruction, provide the best environment for students to learn and ensure student success.
- This data also helps lawmakers make informed decisions regarding education policy and funding.

Rapid Response Tool: Student Data Privacy Newspaper Opinion Pieces

Letter to the Editor

From a superintendent/district administrator or local school board member:
Word Count: 263

Students deserve an environment where their safety and privacy are protected, particularly when it comes to using new technologies and online services.

As leaders of our local schools, we know the community trusts us to protect student data. We are the frontline protectors of sensitive student data, and it is our responsibility to safeguard this information. We take that responsibility very seriously and expect all our teachers, staff and outside service providers to do the same.

[insert name of school district] has a comprehensive student data privacy policy that complies with all federal and state laws designed to keep students' educational records confidential. This policy outlines all of the procedures and security mechanisms we have to protect student data. It also governs who has access to data and how it can be used.

Our school district restricts access to this data to qualified, authorized users only. Strict controls have been placed on any technology partner or outside provider that must access student data in order to perform a necessary service for our schools. Authorized users – be they teachers, school nurses or companies providing math software to our schools – are only given access to the specific pieces of data they need to do their jobs and not to a student's complete record.

Student learning data provides those involved in our students' education with valuable information we need to make smart choices that will help students succeed. With the help of secure, confidential data, the [insert name of school district] can reach our goal of ensuring every student is well prepared for college, a career and life.

Student Data Privacy Newspaper Opinion Pieces – Continued

Letter to the Editor

From our Chief Information Officer:
Word Count: 246

While schools and school districts have always collected data about students – course enrollments, scores on assignments and tests, and daily attendance – management and analysis of this information has increasingly moved to digital formats online. Just as our school buildings need to be safe, students deserve an online environment where their safety and privacy are protected. We at [insert name of school district] expect our employees and partners to protect student data and have created policies and procedures to help prevent the misuse of student data.

Our policies limit who has access to data about students and what types of data they can access. Authorized users such as teachers, school nurses or companies providing math software to our schools are only given access to the specific pieces of data they need to do their jobs. They do not have access to a student's complete record.

Restricting access to only authorized individuals is one of the best ways to protect students' educational records. Our district also makes use of industry-accepted security measures, such as data encryption, firewalls and audits of security practices and user activity.

Additionally, there are federal and state privacy laws specifically designed to protect student data and ensure that schools, districts and education service providers are keeping student data confidential. These include strict penalties if data is misused or compromised. While we live in an increasingly digital world, [insert name of school district] parents should take comfort that we take our responsibility to safeguard student data seriously.

Student Data Privacy Newspaper Opinion Pieces – Continued

Opinion-Editorial (Op-ed)

Proposed Author: Superintendent, district administrator, district CIO or local school board member
Current word count: 408

Gathering accurate and up-to-date data about students and schools is crucial for improving our education system and giving students the best opportunity to succeed. The types of data collected can be indicators of what is and what is not working in our ongoing quest to ensure students are well prepared for the next steps in their education journey, for college and, ultimately, a career.

We want to make sure our students are not only keeping up within our state and country, but also excelling to their fullest potential. This information helps us locally and informs state and national officials on overall trends or developments in education. Legislators also use this information for guidance in policy decisions and budgeting.

While many different groups benefit from knowing student data, not every group can, or should, receive the same data. Our school district has a comprehensive student data privacy policy that sets very clear boundaries on data usage, including who has access to the data and how it can be used.

Our school district's policies restrict access to student data to qualified, authorized users only. And, users are only granted permission to see the subset of data they need to do their jobs. Strict controls have been placed on any technology partner or outside provider that must access student data in order to perform a necessary service for our schools.

Restricting access to authorized users only – whether they are inside or outside the school system – and restricting the types of information they can look is key to protecting student data.

Additionally, our school system uses modern technology to our advantage as another means of keeping student information confidential. Data encryption, secure servers, firewalls, intrusion detection software and logs of user activity all help insulate student data.

And, finally, there are multiple layers of federal and state laws designed to keep students' information private. These existing laws place severe penalties on individuals who misuse data.

As leaders of our local schools, we know the community counts on us to not only keep students safe while they are in our schools, but to also shield students' learning data. We are the protectors of student data and we take that responsibility very seriously. Nothing is more important to us than the safety of your children, the security of their educational information and our efforts to set them on a pathway to success. Visit [insert url] to learn more about our student learning data policies and practices.

Rapid Response Tool: Student Data Privacy Social Media Posts

Facebook

Have you heard all the buzz about #studentdata lately? Our district takes your child's data privacy seriously, and we have adopted privacy and security policies to protect your student. There are also state and federal laws that safeguard the use of student data. Learn more by visiting [insert link to student data privacy page on website]

#StudentData. You've heard about it, but what exactly is it? It's basic information like name, date of birth, address and parent or guardian contact info. It also includes information that teachers, schools and parents can use to make sure students are making progress like test scores, report card grades, attendance and statewide assessment scores. [insert link to or image of infographic]

Access to #studentdata is carefully restricted to authorized users only. Student data is NEVER bought, sold or traded to anyone. That is a violation of state and federal laws. Check out our student data privacy policy to learn more. [insert link to policy]

Our teachers use #studentdata to create personalized learning plans for your child so we can ensure he/she succeeds in school and beyond. [insert link to or image of infographic]

Schools do not collect personal information on parents or guardians like social security numbers or driver license numbers. Schools only collect basic contact information so parents and guardians can be reached in case of an emergency. #studentdata

There are three main types of #studentdata. Personally Identifiable Information, which is information connected to individual students, like name. De-identified Data, which is information about individual students but with no identifying information like name included. And Aggregate Data, which is information on groups of students and does not include any identifiable information on individual students.

Who has the most access to #studentdata? Parents of course! Parents are always in the driver's seat when it comes to their child's information. This infographic explains who else has access and how much access they get. [insert link to or image of infographic]

Student data is protected by our school district and local schools through comprehensive privacy policies and multiple layers of security measures like firewalls, data encryption, secure serves and intrusion detection software. [insert link to or image of infographic]

Student Data Privacy Social Media Posts – Continued

Our school district and schools sometimes hire outside providers to help with critical functions like transportation and management of instructional tools. These outside providers are only granted access to the data they need to do their jobs. Our schools maintain strict control over all access to #studentdata.

#Studentdata is vital to helping your child succeed in the classroom by helping teachers create the right environment for your child to learn. Teachers are trained to protect the student data that they can access. [insert link to student data privacy page on website]

#Studentdata has been recorded for many years on paper, but as we move into an increasingly digital age, much of this data has shifted to online formats. This allows for more accurate and up-to-date sharing of information among teachers, parents and school administrators. [insert link to student data privacy page on website]

Student data provides those involved in our children's education with valuable information we need to make smart choices that will lead to better learning outcomes for students. With the help of secure, confidential data, we can reach our goal of ensuring every student is well prepared for college, career and life. #studentdata

Our schools don't just use student data to help students. It is also used to help teachers see how they're doing. Teachers need to know how they are performing in the classroom. The more they know, the better they can tailor instruction for each student.

Per our school district policy, access to #studentdata is restricted to authorized users only. Users are only given access to the data they need to do their jobs. Read our full Student Data Privacy Policy here [insert link to student data privacy policy]

Twitter

Our district has adopted policies to protect #studentdata, in addition to state and federal laws. Learn more: [insert link to student data privacy page on website] #studentdata

What is #studentdata? This great infographic explains the types of data collected on students. [insert link to or image of infographic]

#Studentdata helps parents, teachers and schools enhance a child's learning experience and ensure success in the classroom and beyond.

We restrict access to #studentdata to authorized users only. Check out our #studentdata privacy policy. [insert link to student data privacy policy]

Student Data Privacy Social Media Posts – Continued

Parents are always in the driver's seat when it comes to their child's information, but who else has access to #studentdata? [insert link to or image of infographic]

Our schools do not collect sensitive information, like social security numbers or parents' and guardians' driver license numbers.

There are multiple federal and state laws that protect #studentdata and prohibit any misuse.

The security of #studentdata is of the utmost importance to our school/school district. Learn how we are keeping your child's info safe. [insert link to student data privacy page on website]

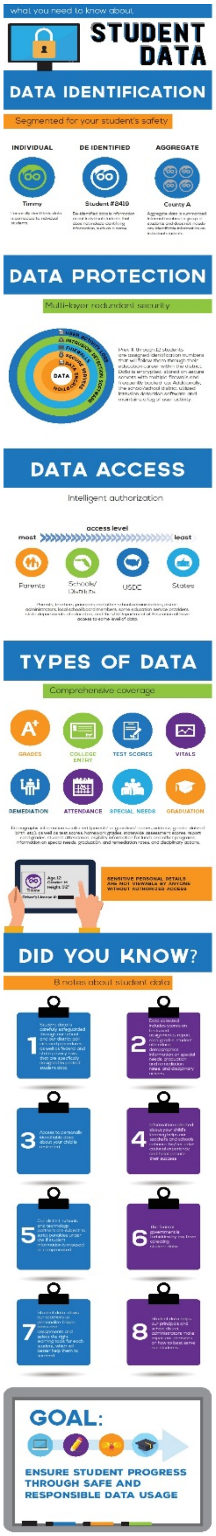
Our students' education records are not and never will be used for marketing or commercial purposes. That is a violation of state & federal law.

Collecting and maintaining #studentdata provides an accurate, up-to-date assessment of how our schools, teachers & students are performing.

#Studentdata enables schools and teachers to personalize learning plans for your child and ensure he/she succeeds in school and beyond.

Toolkit Resources – Graphic Materials

Student Data Privacy Infographic

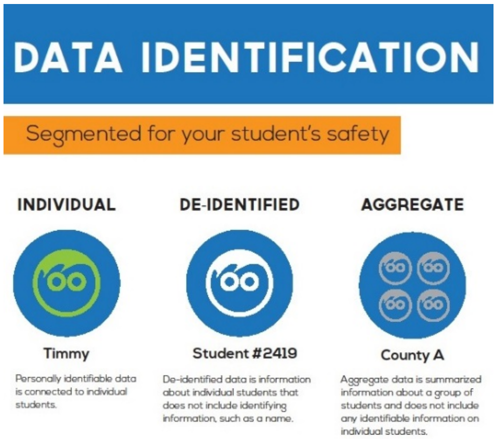

what you need to know about
STUDENT DATA
DATA IDENTIFICATION
Segmented for your student's safety
INDIVIDUAL
DE IDENTIFIED
AGGREGATE
Timmy
Student #2419
County A
DATA PROTECTION
Multi-layer redundant security
USER ACTIVITY LOGS
INTRUSION DETECTION SOFTWARE
FIREWALLS
SECURE SERVERS
DATA ENCRYPTION
DATA
Pre-K through 12 students are assigned identification numbers that will follow them through their education career within the district. Data is encrypted, stored on secure servers with multiple firewalls and frequently backed up. Additionally, the school/school district utilizes intrusion detection software and maintains a log of user activity.
DATA ACCESS
Intelligent authorization
access level
most
least
Parents
Schools/ Districts
USDC
States
Parents, teachers, principals and other school administrators, district administrators, local school board members, some education service providers, state departments of education, and the US Department of Education all have access to some level of data.
TYPES OF DATA
Comprehensive coverage
GRADES
COLLEGE ENTRY
TEST SCORES
VITALS
REMEDIATION
ATTENDANCE
SPECIAL NEEDS
GRADUATION
Demographic information is collected (parents'/guardians' names, address, gender, date of birth, etc.), as well as test scores, homework grades, statewide assessment scores, report card grades, student attendance, eligibility information for lunch and other programs, information on special needs, graduation, and remediation rates, and disciplinary actions.
Age 12
Gender M
Height 5'2"
Timmy
Driver's License #
SENSITIVE PERSONAL DETAILS ARE NOT VIEWABLE BY ANYONE WITHOUT AUTHORIZED ACCESS
DID YOU KNOW?
8 notes about student data
1 Student data is carefully safeguarded through our school and our district policies and procedures, as well as federal and state privacy laws that are specifically designed to protect student data.
2 Data collected includes scores on tests and assignments, report card grades, student attendance, demographics, information on special needs, graduation and remediation rates, and disciplinary actions.
3 Access to personally identifiable data about your child is restricted.
4 Information collected about your child's learning helps our teachers and schools enhance his/her educational experience and help ensure their success.
5 Our district, schools, and technology partners are subject to strict penalties under law if student information is misused or compromised.
6 The federal government is prohibited by law from collecting student data.
7 Student data allows our teachers to personalize lesson plans and assignments and select the right learning tools for each student, which will better help them to succeed.
8 Student data helps our principals and school district administrators make important decisions on how to best serve our students.
GOAL:
ENSURE STUDENT PROGRESS THROUGH SAFE AND RESPONSIBLE DATA USAGE

Student Data Privacy Web & Social Media Banners

Privacy
STUDENT
DATA
PRIVACY

STUDENT
DATA
PRIVACY

Student Data Privacy Other Graphics



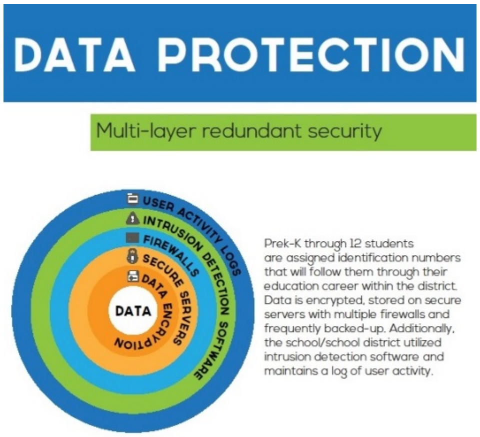
DATA IDENTIFICATION

Segmented for your student's safety

Personally identifiable data is connected to individual students.

De-identified data is information about individual students that does not include identifying information, such as a name.

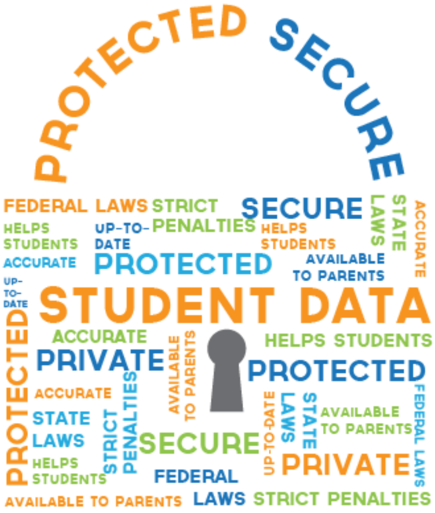
Aggregate data is summarized information about a group of students and does not include any identifiable information on individual students.

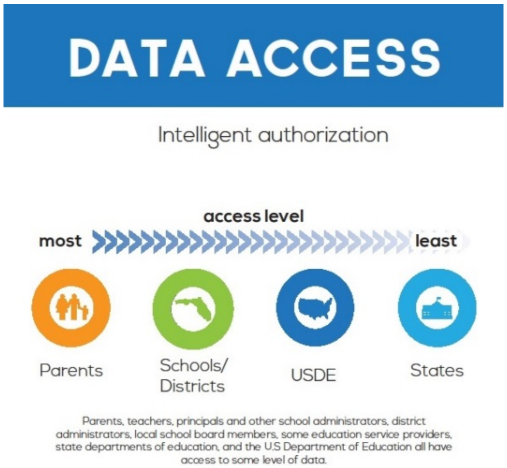


DATA PROTECTION

Multi-layer redundant security

Prek-K through 12 students are assigned identification numbers that will follow them through their education career within the district. Data is encrypted, stored on secure servers with multiple firewalls and frequently backed-up. Additionally, the school/school district utilized intrusion detection software and maintains a log of user activity.

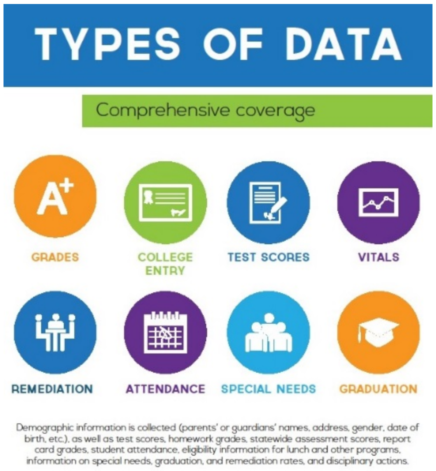




DATA ACCESS

Intelligent authorization

Parents, teachers, principals and other school administrators, district administrators, local school board members, some education service providers, state departments of education, and the U.S Department of Education all have access to some level of data.



TYPES OF DATA

Comprehensive coverage

Demographic information is collected (parents' or guardians' names, address, gender, date of birth, etc.), as well as test scores, homework grades, statewide assessment scores, report card grades, student attendance, eligibility information for lunch and other programs, information on special needs, graduation, and remediation rates, and disciplinary actions.

Additional Resources

Many organizations actively advocate for student data privacy policies that on one hand build trust and empower parents; while on the other provide teachers, school leaders, policymakers and innovators with information that can spur student achievement. These organizations provide a wealth of information that, in addition to the resources provided above, assist state leaders and education stakeholders to better communicate with parents and teachers on this important issue. See below for a nonexclusive list of helpful resources for districts and parents.

Best Practices for Student Data Privacy Policies

- 10 Steps Districts Should Take Today, COSN
- Protecting Privacy Toolkit, COSN
- Making Sense of Student Data Privacy, Bob Moore
- Student Data Principles, DQC and COSN

Additional Information for Parents

- Parent's Guide to Student Data Privacy, FERPA|SHERPA
- Who Uses Student Data Infographic, DQC
- What is Student Data Infographic, DQC
- What is Student Data Video, DQC
- Talking about the Facts of Education Data with Parents, DQC
- What Every Parent Should Be Asking about Education Data and Privacy, DQC
- Myth Busters, DQC
- Clear Privacy Practices, COSN

Additional Information for School Districts

- Student Data Collection, Access, and Storage, DQC
- A Stoplight for Student Data Use, DQC
- Talking about the Facts of Education Data with Policymakers, DQC
- Cheat Sheet: Data Privacy, Security, and Confidentiality, DQC
- School Officials, FERPA|SHERPA
- Federal Laws, FERPA|SHERPA
- FERPA exceptions, PTAC

Resources for Communicating Why Data is Important

- Empowering Parents with Data, DQC
- Data: The Missing Piece in Improving Student Achievement, DQC

Resources on Actions by Service Providers and Vendors to Protect Student Data Privacy

- Student Privacy Pledge, FPF and SIIA

ExcelinEd

Stay Connected

EXCELINED.ORG

FACEBOOK.COM/EXCELINED

@EXCELINED