

Doug Webb, General Counsel
The School District of Greenville County
2025

National Data Breaches

- NBC News Article: Children's data hacked after school software firm (Powerschool) missed basic security step, internal report says
 - An executive admitted during a meeting that a breached account had failed to use multi-factor authentication, according to materials reviewed by NBC News.

School Specific Data Breaches

- BY VERL JOHANSEN AND DIANA JONES
- KSLNewsRadio
- SALT LAKE CITY The <u>Granite School District</u> has experienced a large data breach.
- The Granite School District confirmed the data breach happened about a month ago.
 The district alerted parents and staff as soon as they found out. Officials are still
 investigating how and what type of data was taken.
- One cybersecurity expert said he found some of that data on the dark web.
- George Kounalis has worked in cybersecurity for four years. He said in his free time he keeps an eye on the dark web to see what types of data hackers are going after.
- He was able to find 14 archived files from the Granite School District that totaled to over two terabytes of stolen data.

A Personal Story



Laws Governing Student Privacy

- FERPA Family Educational Rights & Privacy Act
- COPPA Children's Online Privacy Protection Act
- PPRA Protection of Pupil Rights Amendment
- FOIA Freedom of Information Act (S.C. law)

Family Educational Rights & Privacy Act

Origin & Purpose of FERPA

- FERPA was enacted in 1974 as part of a bill extending the Elementary and Secondary Education Act of 1965.
- Designed to protect the rights of students and parents
 - Assures access to educational records
 - Prevents disclosure of personally identifiable student information unless an exception exists in FERPA.

Technology in 1974





The Cloud in 1974



Cell Phones in 1974



FERPA Fundamentals

Rights for Parents & Eligible Students

- FERPA initially protects the rights of parents
- These rights are then transferred to students at the age of 18 or when the student attends a learning institute beyond high school
- Parents and eligible students have the right (among others) to...
 - Inspect and review the individual's education records maintained by the school
 - Request that a school correct records which they believe to be inaccurate or misleading

Student Record

- Student record contains files, documents, and other materials which have information that is...
 - DIRECTLY related to the student
 - Information must be personally identifiable in order for it to be considered protected information
 - MAINTAINED by an educational agency or institution

Two Parts of a Student Record

- Student record information can be placed into two categories defined under FERPA. Both have different disclosure protections.
 - (1) Directory Information
 - Can be disclosed without written consent, unless student specifically requests information to be withheld
 - Name, Address, Pictures, Degree Awarded, Enrollment Status, etc.
 - Administrative Rule JR Defines District's Directory Information
 - (2) Non Directory Information
 - Can **not** disclose without written consent
 - Race, Transcripts, SSN, Personally Identifiable Information (direct or indirect identifiers)

Exceptions

- Student records can be released without consent to the following parties or under the following conditions:
 - Other schools to which a student is transferring
 - Specified officials for audit or evaluation purposes
 - Appropriate parties in connection with financial aid to a student
 - Organizations conducting certain studies for or on behalf of the school
 - Accrediting organizations
 - To comply with a judicial order or lawfully issued subpoena
 - Appropriate officials in cases of health and safety emergencies
 - School officials with legitimate educational interest
 - State and local authorities, within a juvenile justice system, pursuant to specific State law

School Official Exception

- School Districts must provide annual notice of the individuals/entities who are designated as "school officials" pursuant to FERPA
- These individuals/entities must be providing services that are necessary for operations and would otherwise be performed by school employees
- School Districts must have a written agreement in place detailing the control of personally identifiable information

School Resource Officer (SRO)

- GCS designates law enforcement officers (SROs) as "school officials" for purposes of disclosing student information when there is a "legitimate educational purpose" and District still controls dissemination of that information. SRO must still comply with FERPA & District policy.
- SROs are not school disciplinarians should not request SRO to intervene in school discipline matters unless student's behavior amounts to a violation requiring law enforcement involvement
- SROs shall be called to respond to any misconduct when:
 - (1) The conduct is criminal, or
 - (2) The conduct presents an immediate safety risk to one or more people SC Reg 43-210

Law Enforcement Access to Records

- Remember that exigent circumstances for time sensitive criminal investigation/protection of safety is an exception to FERPA restrictions and law enforcement can have records and see/receive video footage from school
 - If law enforcement is investigating a criminal case without exigent circumstances then a subpoena is required
- Attempt to cooperate with law enforcement to extent possible
- See Administrative Rule JCAB Students: Searches, Interrogations, and Arrests

DSS Case Workers & Guardians Ad Litem Access to Students

- School principals should cooperate with DSS case workers and properly appointed guardians ad litem in their investigations of suspected child abuse.
- The need to cooperate does not alter the rules of confidentiality of student records set forth in Policy JR for DSS unless DSS has custody of child.
- Guardian Ad Litems can obtain student records with court order.
- See Rule JGI Students: Student Welfare: Child Abuse

FERPA Annual Notice

- FERPA requires the District to <u>annually</u> provide notice to parents and eligible students that the District may disclose "directory information" without consent if it has given public notice to parents and eligible students of the:
 - types of personally identifiable information it has designated as directory information,
 - right to restrict the disclosure of such information ("opt-out"), and
 - period of time within which a parent or eligible student has to notify the District that he or she does not want any or all of those types of information designated as directory information.

Emails & Surveillance Videos and FERPA

- District's position is that emails and surveillance videos involving students are <u>not</u> maintained by the District as part of a student's educational record and are therefore <u>not</u> subject to FERPA...
 - ... unless...either placed in a student's educational record as part of a disciplinary matter or for another valid reason.
- However, disclosure of emails and videos may be required pursuant to a valid FOIA request.
- For *video recordings*, see Administrative Rule EB (Building & Grounds Management)

Data Breaches & Preventative Steps

PowerSchool ("School Official") Data Breach

- PowerSchool is considered a "school official" for FERPA purposes
- Nation-wide breach affecting millions of students ---breach lasted for approx. a week
- Foreign threat actor accessed PowerSource, which is a support portal for PowerSchool that had remote access to school districts
- Affected most school districts in South Carolina

PowerSchool Breach Cont.

- Greenville County Schools was not affected with three practices that helped avoid the breach
 - GCS requirement of supervised remote access
 - Firewalls are more protective and prevent foreign internet traffic
 - Utilization of 2 Factor Verification System

Data Sharing Agreement

- Notification Language: Entity shall immediately report to District any suspected breach of confidentiality of Information or a violation of any term of this Agreement and take immediate steps to limit and mitigate such security breach to the extent possible. Entity agrees that any breach of the confidentiality obligation set forth in the contract may, at District's discretion, result in cancellation of further consideration for contract award and the eligibility for Entity to receive any information from District for a period of not less than five (5) years. In addition, Entity agrees to indemnify and hold the District harmless for any loss, cost, damage or expense suffered by District, including but not limited to the cost of notification of affected persons, as a direct result of the unauthorized disclosure of education records.
- FERPA & SC Section 1-11-490 Notification Obligations

Data Breach Notification

- If only FERPA protected information, the law requires you to denote in the affected student's record the breach- practically should contact parent/guardian as well.
- If more sensitive information such as name coupled with date of birth or address (or other more sensitive information), then it is a violation of state law and more defined notification procedures are required

Data Sharing Agreement

• Indemnification Language: Entity agrees to the fullest extent permitted by law to hold harmless, defend, and indemnify District, its agents, employees and trustees from any liability, cost, or expense, including without limitation penalties, losses, damages, attorneys' fees, taxes, expense of litigation, judgments, liens and encumbrances, to the extent arising out of or resulting from any act or omission by Entity pursuant to this Agreement.

District process for approval of vendors and educational apps?

Process for Approval of Vendors

 Process for Approval of Educational Apps & Online Programs

Process for Approval of Access to District Information and Programs by a Third Party (Vendor)

This process is only necessary when personally identifiable information, including, but not limited to, student or employee information is accessible by a third party who has entered into an agreement to provide support to the District. Personally identifiable information includes direct identifiers, such as a name or indirect identifiers, such as a date of birth, or other information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

The department (i.e. Academics, Human Resources, etc) interested in contracting with a
vendor must fully review the proposed relationship and potential support provided by that
vendor. Examples of such support can be to provide assistance to the District for
employee payroll programs, provide mental health counseling in schools, or provide
athletic training services to students.



2. If the department's supervisor supports moving forward with a vendor, that supervisor, after consulting with the Deputy Superintendent, will contact the Legal Department to review any agreement of terms and conditions (master agreement) between the parties and will also contact ETS to complete a Data Sharing Agreement.



3. If the services provided by the third party require access to a District program, such as Powerschool, or the use of a District email address, a Vendor Access Agreement must be completed by the individual employees of the vendor who will be provided access to a District program or the use of District email. (See Attached Agreement).



4. ETS will retain all Data Sharing Agreements and Vendor Access Agreements in accordance with District information retention procedures.



5. The department requesting the support of the vendor will retain and upload the master agreement and any Vendor Access Agreements in the Access Management System (AMS) to ensure appropriate access by other District employees.

Process for Approval of Educational Apps and Online Programs

This process is only necessary when personally identifiable student information is entered into an app or program. Personally identifiable information is student information that is maintained in education records and includes direct identifiers, such as a student's name or indirect identifiers, such as a student's date of birth, or other information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. Please contact ETS if you are unsure whether the app or program requires personally identifying information.

- The school's administration needs to fully review and consider the educational value of the app or program.
- If the school's administration finds that the app or program should be used for student learning, the school will contact Academics to review. (Principals need to click on the following link and fill out the form for approval of educational apps) Request Form



 If Academics approves of the app or program, Academics will contact ETS to ensure compliance with the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA). ETS will review the app or program to ensure that no technology-related concerns exist.



ETS will contact the Legal Department to approve any master agreement or any Data Sharing Agreement (if it deviates from the approved template).



5. ETS will notify Academics and School of the approval of the app or program.



ETS will include the app or program on the District's website as a means of notification for both
parents and schools at https://www.greenville.k12.sc.us/Parents/main.asp?titleid=coppa. ETS will
retain the Data Sharing Agreement and the Master Agreement (or Terms of Use) for each app or
program.

Greenville County Schools Policy/Rule JR

Regarding Student Privacy

Greenville County Schools Policy JR Regarding FERPA

The district will notify parents/legal guardians and eligible students of the following rights:

- Right to inspect and review the student's educational records
- Right to receive an annual public notice of parents and eligible student's rights and opportunity to opt out of the release of directory information
- Right to request the amendment of the student's educational records
- Right to receive a response to reasonable requests for explanation and interpretation of the educational records
- Right to receive copies of educational records if circumstances effectively prevent the parent or eligible student from exercising the right to inspect and review the student's educational records
- Right to request a hearing to correct an incorrect record or other violation of FERPA

Greenville County Schools Rule JR Regarding FERPA

Rule JR encompasses

- Location of Student Records
- Management of Records
- What qualifies as directory information
- Disclosure
- Request for Inspection of Records
- Hearings to Challenge Information in Student Records
- Destruction of Student Records
- Transcripts

Rule JR Request for Inspection of Records

- Right to Inspect
 - Anyone who wishes to inspect records must make a request for inspection to the principal of the school in which the student is enrolled or where the record is housed.
 - Principals or the Superintendent's designee will set a time and place for inspection of records within 45 days after the request has been made (should do it as soon as reasonably possible---usually a few days)
 - If a hearing concerning student is pending, the employee will honor the request for inspection prior to the hearing.

Rule J-JR Right to Appeal

- Right to Appeal
 - If parent/guardian or eligible student believes that the information in the record is inaccurate, misleading or violates the privacy or other rights of the student, they can request an amendment to the record.
 - The District will amend the record if appropriate or notify the parent/guardian or eligible student within 15 working days in writing that the request was denied. The individual then has the right to request a hearing.

Administrative Rule JR Hearing Process

Hearing Process

- Parent/ legal guardian or eligible student will make a request for hearings to the principal where the record is housed. The principal or his/her designee may conduct the hearing.
- Principal/administrator will set a date, time, and place for hearing and notify requester in writing of the date, time, and place.
- Hearing will occur within 15 working days of receipt of the request.
- The parent/legal guardian or eligible student will have full and fair opportunity to present relevant evidence and may be assisted at their expense by legal counsel.
- If the District finds that the information is not inaccurate or in violation of the privacy rights, it will inform parent/guardian or eligible student in writing that he or she has the right to place a statement commenting upon the disputed information in the record.
- If the District finds that the information is incorrect, the District will correct any mistake.
- The District will send its decision and a summary of the evidence and the right to a judicial appeal in writing to the parent/guardian or eligible student within 15 working days after the hearing.

Children's Online Privacy Protection Act

(COPPA)

Origin & Purpose of Children's Online Privacy Protection Act (COPPA)

- Enacted by Congress in 1998
- Federal Trade Commission (FTC) issues & enforces regulations concerning children's online privacy.
- Primary purpose is to place parents in control over what online information is collected, used, and disclosed from their children under age 13

COPPA & Schools

- District can contract with 3rd party website operators for online programs and for educational benefit of students.
- The school may act as the parent's agent for consent only where an operator collects personal information from students for the use and benefit of the school.
- Cannot use student information for commercial purposes; that use requires specific parental consent.
- Follow District procedures for Process of Approval for Educational Apps

Operators Covered by the COPPA Must:

- Post a clear & comprehensive online privacy policy (also sent home to parents)
- Post a list approved programs
 - https://www.greenville.k12.sc.us/Parents/main.asp?titleid=coppa
- Maintain confidentiality, security, and integrity of collected information
- Collection of information is for only as long as necessary to fulfill purpose & delete using reasonable measures to protect against unauthorized access/use

Protection of Pupil Rights Amendment (PPRA)

Purpose of PPRA

- Governs the administration of a survey, analysis, or evaluation to **students** that concerns one or more of the following protected areas:
 - Political affiliations or beliefs of the student or parent;
 - Mental or psychological problems of the student/family;
 - Sex behaviors or attitudes;
 - Illegal, anti-social, self-incrimination, or demeaning behavior;
 - Critical appraisals of close family relationships;
 - Legally recognized privileged relationships;
 - Religious practices, affiliations, beliefs of student/parent; or
 - Income (other than to determine program eligibility).
- Board Policy JKA details rights pursuant to PPRA, including the ability for parents to inspect surveys, instructional materials, and the prohibition of certain surveys without prior parent consent.

Freedom of Information Act (FOIA)

Freedom of Information Act (FOIA)

- A person has a right to inspect, copy, or receive any <u>public record</u> of a <u>public body</u>, except...(key exceptions below)
 - Information of a personal nature where the public disclosure would constitute unreasonable invasion of personal privacy.
 - Records or videos compiled for law enforcement purposes
 - Matters specifically exempted from disclosure by statute or law
 - Materials gathered by the public body during a search to fill an employment position except materials relating to the final three applicants
- S.C. Code of Laws § 30-4-10 et seg

What must be disclosed under FOIA?

- Emails between school employees regarding a specific student?
- Student discipline records?
- District surveillance video of a fight between students at a school?
- Employee personnel records?
- Be **very cautious** about what you write and send by email. Could be subject to disclosure in accordance with FOIA, and if there is litigation, through subpoenas and the discovery process.