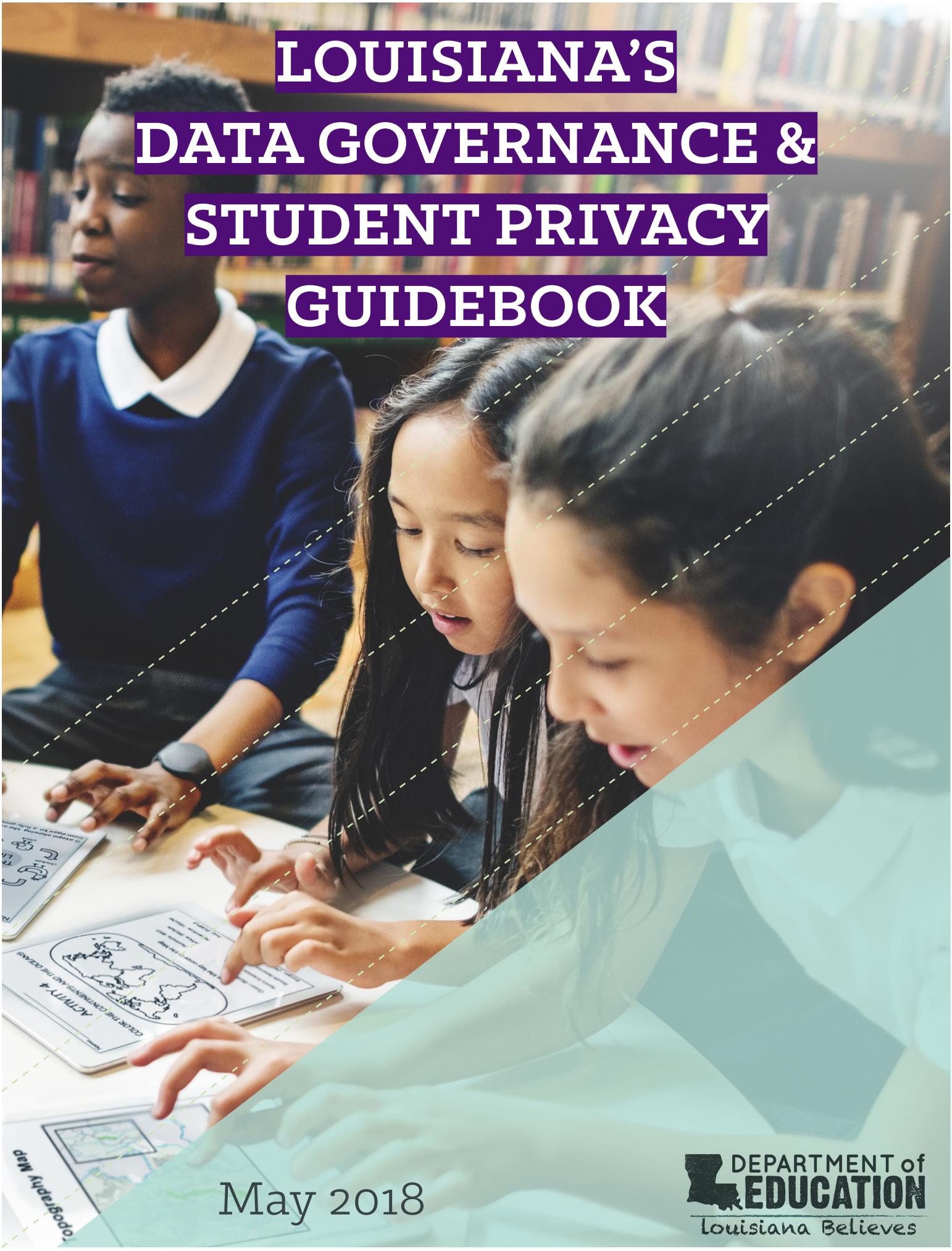
LOUISIANA'S DATA GOVERNANCE & STUDENT PRIVACY GUIDEBOOK



May 2018

DEPARTMENT of EDUCATION
Louisiana Believes

CONTENTS

INTRODUCTION 1

ESTABLISH A DATA GOVERNANCE 2

AND PRIVACY ACTION PLAN 2

STEPS FOR ESTABLISHING A DATA GOVERNANCE AND PRIVACY ACTION PLAN 2

Step 1: Know the Laws 2

Step 2: Build a Team 3

Step 3: Provide Training 4

Step 4: Build Strong Protocols 4

Step 5: Make Security a Priority 6

Step 6: Involve Parents 8

APPENDIX A – TERMS TO KNOW 10

APPENDIX B – LAWS IN MORE DETAIL 11

The Children's Internet Protection Act (CIPA) 11

The Children's Online Privacy Protection Act (COPPA) 11

Family Educational Rights and Privacy Act (FERPA) 12

Protection of Pupil Rights Amendment (PPRA) 12

Louisiana's Student Privacy Law (R.S. 17:3914) 13

R.S. 17:3913 13

R.S. 17:112 13

This public document was published at a cost of $539.00. One hundred fifty (150) copies of this public document were published at this first printing at a cost of $539.00. The total cost of all printings of this document, including all reprints, was $539.00. This document was printed by OTS-Production Support Services, 627 North 4th St., Baton Rouge, LA 70802 for the LA Department of Education to provide guidance for establishing data governance at the LEA and school levels. This material was printed in accordance with the standards for printing by State agencies established pursuant to R.S. 43.31.

INTRODUCTION

Data is a crucial component in educational success. It gives each of us the power to address student needs, study what strategies work, and make necessary changes so that every student has the greatest opportunity.

DATA = SUCCESS

Teachers need data to understand when students are thriving and when they need more support in learning specific concepts.

Parents and guardians need access to their child's educational data to help them succeed.

Students need feedback on their progress so they can make good decisions about program choices and prepare for success.

School Officials and community members need to understand school performance and know if education resources are being allocated fairly and effectively.

Today, educators, parents, and students have access to more data than ever before and have access to more technology tools to facilitate the use of data. Accordingly, stakeholders have increased concerns for student privacy that have resulted in new laws and policies to ensure student data is protected. To continue using data to reach educational success, increased privacy, safeguards, and transparency are necessary. A system of data governance accomplishes this by designating rules, procedures, and groups responsible for decision-making regarding data collection, use, and access.

Louisiana's Data Governance and Privacy Guidebook provides a framework for establishing data governance at the local educational agencies (LEA) and school level. It attempts to offer best practices, action steps, and responsibilities regarding data governance and student privacy; however, it is not intended to provide legal advice, and the laws referenced in this guidebook may not be exhaustive. LEAs and schools should contact their legal counsel for any questions or concerns about laws, policies, and practices regarding protection of student privacy and the sharing of student information and data.

ESTABLISH A DATA GOVERNANCE AND PRIVACY ACTION PLAN

Educators across Louisiana are committed to ensuring the privacy, security, and confidentiality of student data while enabling that information to be used to improve student outcomes. To accomplish this goal, each level – the Louisiana Department of Education (LDOE), LEAs, and schools – need a system of governance based on the applicable laws, focused on clear communications and transparency, and that addresses policies, processes, and best practices. The action steps below can be used to develop a data governance and privacy action plan that will result in a customized system of data governance.

STEPS FOR ESTABLISHING A DATA GOVERNANCE AND PRIVACY ACTION PLAN

Step 1: Know the Laws	Laws provide a baseline of protections for students and families.
Step 2: Build a Team	Who should be on the data governance and privacy team? Who should be building privacy policies and practices?
Step 3: Provide Training	Use education of all stakeholders as the foundation of the plan.
Step 4: Build Strong Protocols	Adopt norms and policies for all data and technology use and for managing contractors, apps, and devices. Implement workable processes.
Step 5: Make Security a Priority	Hold all data users and managers accountable. Establish legally binding agreements to hold contractors accountable are established. Ensure data systems, networks, and devices are protected from cyber threats.
Step 6: Involve Parents	The ability to communicate and build trust with parents is essential. Empower families to help take charge of their children's education.

STEP 1: KNOW THE LAWS

Privacy laws provide the baseline for data governance and privacy policies by establishing minimum protections for protecting students' personally identifiable information (PII). These laws establish the definition of personally identifiable information and the guidelines surrounding the sharing of such information.

Federal Laws

- **Children's Internet Protection Act (CIPA)** requires Internet safety policies such as technology to block certain access, monitoring of access, and programs to educate students on appropriate online behavior.
- **Children's Online Privacy Protection Act (COPPA)** assures that children under 13 years of age do not share personal information on the Internet without the express approval of their parents.
- **Family Educational Rights and Privacy Act (FERPA)** regulates the release of personally identifiable information, including parental rights regarding notification of the release of records.
- **Military Recruiters** – **The Elementary and Secondary Education Act of 1965 (ESEA)** requires local educational agencies (LEAs) receiving assistance under the ESEA to provide military recruiters with directory information (specifically names, addresses, and telephone listings) unless parents have opted out.
- **Protection of Pupil Rights Amendment (PPRA)** establishes requirements related to parental notification and opt-out option when collecting information from students that may be used for marketing purposes or when administering surveys or physical exams/screenings.

Louisiana Laws

- **Louisiana's Student Privacy Law** – **LA R.S. 17:3914** (Act 837 of 2014) requires LEAs to assign unique identifiers to all students and to collect and track parental consent to share PII with BOR and LOFSA. Louisiana's student privacy law also provides for limitations on the collection and sharing of student information.
- **LA R.S. 17:3913** (Act 677 of 2014) requires LEAs to make available at the main office of the governing authority, information about any sharing of students' personally identifiable information.
- **Transfer of Student Records** – **LA RS 17:112** mandates the transfer of student records upon the written request of any authorized person on behalf of a public or nonpublic school within or outside the state of Louisiana where the student is seeking enrollment, or an educational facility within a correctional or health facility within or outside the state of Louisiana where the student is seeking enrollment. The transfer of such records, whether by mail or otherwise, must occur no later than ten business days from the date of receipt of the written request.

Put Into Action

School Board Privacy Policy	• Determine type of parental consent – "explicit" or "implied" (**LA R.S. 17:3914**). • Determine what elements will be considered directory information (**FERPA**).
Parental Notification	Conduct an annual notification period where parents are notified of • Parental rights under **FERPA** and **PPRA**, • Any collection of information under specified events as outlined in **PPRA**, • The adopted school board privacy policy, and • The opportunity to not participate (or participate) in information being shared via school directory, online services, surveys, screenings, or marketing.
Parental Consent	Collect parental consent for • Any online services that collect student information for instructional purposes (**COPPA**), • Louisiana Office of Student Financial Assistance (LOSFA) and Board of Regents (BOR) (**LA R.S. 17:3914**), and • Any other applicable programs where student information is shared (**LA R.S. 17:3914**).
Technology Responsibilities	Assess technology filters, provide safety education, provide public notice, and institute acceptable use policies and Internet monitoring policies (**CIPA**).
Data Release	Establish processes to respond to requests from military recruiters and school systems in a timely, secure manner.

STEP 2: BUILD A TEAM

For data governance to be effective, most stakeholders should be represented. Representatives may include data staff who manage student information, IT staff, school administrators, counselors, teachers, and parents.

Depending on the size of school or LEA, multiple teams may need to be established to be responsible for various elements of the data governance plan. These teams may include online services review board, LEA privacy policy development, and data breach response team. The governance team will help develop policies and practices that are right for the LEA or school.

STEP 3: PROVIDE TRAINING

Team members and the school community will need to be trained on data governance and student privacy, and that training will depend on their role.

AUDIENCE	TOPICS
Data Staff, Information Technology Staff	• **Legal and ethical responsibilities** • **Disclosure avoidance techniques** • **Policies and Processes** • **Security**
Teachers and Counselors	• **Legal and ethical responsibilities** • **Best practices** • **Policies and processes**
Students	• How to protect personal information • Selecting good passwords and password protection • Cyberbullying • For additional topics, please see **Louisiana's Guide to Digital Literacy** Tools for training students on the above topics: **Common Sense Media**, **OnGuardOnline - FTC**, **Net Smartz**

STEP 4: BUILD STRONG PROTOCOLS

There are many best practices in the area of data governance and privacy. In this guidebook, the LDOE has provided several examples, however this is by no means an extensive list. The LDOE encourages LEAs and schools to reach out to **LDEData@la.gov** for more information about the data governance plans being implemented across the state.

Online Services

Be cautious of "free online services"; they may introduce security vulnerabilities into the network. It is important to develop policies to govern the use of free services. Establish a team to review the online services available and the risks they pose. Use that analysis to determine which services will be most useful with the lowest possible risk of disclosing personally identifiable information of students.

Click-wrap or click-through agreements are when an end-user enters into an agreement by clicking "OK" or "AGREE," and are very unlikely to have actually read through the entirety of the agreement presented. When using an online tool that relies on a click-wrap agreement:

- *check amendment provisions,*
- *print and save the terms of service,*
- *develop a policy for use of these types of tools, and*
- *develop a list of approved tools.*

Third Party Contracts or Data Sharing Agreements

RS 17:3914 (C) states that "a city, parish, or other local public school board may contract with a public or private entity for student and other education services, and pursuant to such contract, student information, including personally identifiable information and cumulative records, may be transferred to computers operated and maintained by the entity for such purpose." Contracts should include the following elements:

- What data will be collected (data)
- Why the data will be collected and how it will be used (purpose of disclosure)
- How the data will be protected (confidentiality , restrictions on use)
- How security audits will occur (security audits)
- How security breaches and notification of security breaches will be addressed (security breach)

See St. Tammany sample contract language

The LDOE has established agreements for statewide services such as assessments. LEAs have the opportunity to opt into these agreements by signing an addendum listed on the **Student Privacy Data Sharing section** of the Louisiana Believes website. These addenda will be kept on record by the LDOE, and also should be kept on record with the data governance team.

Disclosure Avoidance and Suppression Techniques

When LEAs, schools or the LDOE release reports publicly, it is important to ensure that students cannot be identified. Aggregated data minimizes the risk of disclosure; however, some risk remains (see two scenarios). Below are some considerations when releasing data.

Sensitive PII is PII that if accessed or released the individual could experience an adverse impact (e.g., social security number, name and mother's maiden name).

The risk of re-identification must be considered. It's unlikely that a student's identity could be derived from a state level report on the counts of students expelled; however, if the report contains the LEA, the school, and the grade level the risk that the student might be identified a member of the community increases.

Staff Best Practices

By following the best practices outlined below, educational communities can ensure students' personally identifiable information is guarded, thereby protecting their right to privacy:

- **Protect visibility** of reports and computer monitors when displaying and working with confidential information.
- **Lock or shut down workstations** when left unattended for any amount of time.
- **Store data in a secure location.** Physical data (including hard copies of reports, storage media, notes, backups) should be protected from unauthorized persons, or locked away when not in use.
- **Transmit sensitive data securely.** This may be done using Secure File Transfer Protocol (sFTP) or encrypted email. Faxing confidential data is not recommended since it poses many security risks.
- **Stamp or otherwise mark confidential** reports or media containing confidential information prior to their release. The envelope containing the information should also indicate that the contents are confidential.
- **Protect user names and passwords:** If using an online educational program which establishes individual log-in information for students such as usernames and passwords, keep them in a private, secure location and teach students to keep their personal log-in information private.

Two Personally Identifiable Disclosure Scenarios

- *An online bully has decided to attack students who have failed state tests. To identify targets, he submits a data request for all assessment results by grade level and subgroup in every school in the state. If any school has 100 percent of students within a grade or subgroup score below proficient, he searches for them on Facebook and sends hurtful messages.*
- *The court has removed the custody rights of an abusive parent, and, therefore, the parent no longer has access to the student's academic results. The parent makes a data request for the all of the Algebra I end-of-course results by race at his son's high school knowing that his son is the only student of a particular race in the ninth grade. He is unhappy about his son's assessment result and plans to wait for him outside of school.*

Policies

LEAs and schools should codify protocols and best practices in the policies they establish. Doing so will provide structure for data governance and privacy goals, establish clear directions, and set clear expectations. Below are some recommended policies for a data governance action plan.

POLICY	PURPOSE	AUDIENCE
Acceptable Use Policy	Establishes how individuals should interact with technology and data *Samples:* • Ascension Parish School Board • NCES	Students and Staff
Online Services Policy	A policy or process for determining which online services will be used in the classroom	Staff
School Board Privacy Policy	A policy established to define how student data will be protected	All

With every policy it is important to ensure monitoring compliance and tracking use. Below are some tools that might be helpful to follow through with established expectations.

Tools to Support Policies and Procedures

- Data Access Tracker
- Data Release Checklist
- Auditing Access Document
- MOU Routing Template

STEP 5: MAKE SECURITY A PRIORITY

Education information technology (IT) systems have increasingly become the target of cyber attacks. Authorities report more and more children's information is being used to make fraudulent documents. Additionally, reports show that one in five educational institutions has been hit and that schools have the highest rate of ransomware attacks of any industry. Hackers look for any opportunity to exploit institutions, and school systems are considered easy targets.[1] While the investment in cyber security can feel burdensome, with the average remediation cost of $245 per record, IT security prioritization is necessary.

Preemptive Actions Resulting in Savings

Organizations can reduce costs in the event of a data breach by taking the following preemptive steps.

- *Maintaining an incident response team and plan: resulting in a savings of $19 per record.*
- *Data encryption: resulting in a savings of $16 per record.*
- *Strong user training programs: resulting in a savings of $12.50 per record.*

Security Recommendations

There are many resources to assist school systems in developing a comprehensive security program. These documents can be very detailed and technical. Below are the basic security considerations.

1. **Access:**
   a. Control access to data systems through strong passwords and multiple levels of user authentication.
   b. Establish and maintain role-based permissions (least amount of access possible to complete job duties).
   c. Encrypt sensitive data when it is stored and transmitted.
   d. Separate student and administrative networks from one another as well as the student information system.
   e. Ensure that all server rooms are secured at all times with controlled access for authorized personnel only. All network, server, and infrastructure equipment should be secured.
   f. Ensure all websites are secured with a digital certificate.
   g. Ensure that all access to systems is logged and audited annually.
   h. Require staff to password encrypt mobile devices that can access school system technology resources.
2. **Maintenance:**
   a. Keep hardware and software patches current.
   b. Maintain effective and current antivirus.
   c. Utilize up-to-date firewalls.
   d. Implement a backup program that is protected from ransomware attacks.
   e. Continuously assess and remediate vulnerabilities regularly.
3. **Training:**
   a. Train staff on how to develop effective passwords and enforce a password change policy.
   b. Most school systems are able to automatically force lockdown of a staff person's computer after it has been sitting idle for a certain amount of time. There is still a danger, however, that students can quickly access a teacher's computer the minute a teacher has stepped out of the room. Remind teachers to lock their computers if they need to step away, particularly while students are present.
   c. Never use unencrypted email to discuss student-level data. To communicate with others outside the firewall, or in an otherwise unsecure exchange, use a password-protected spreadsheet and send the password in a separate communication.
   d. Before leaving working areas, sensitive documents should be secured. Ensure a clean-desk policy.
4. **Incident Response Planning**
   a. Develop an incident response team with each member holding specific responsibilities in the event of an incident.
   b. Complete the **Incident Response Plan and Reporting Template** to establish the steps to take in the event of an incident.
   c. If an incident occurs, record the steps taken using the Incident Response Plan and Reporting Tool.
   d. Review the Incident Response Plan at least once annually.

Reports show that 90% or more of cyber-attacks are caused by human error or behavior. Many times malware, software designed to damage a computer, or ransomware, software designed to hold a computer's functionality and/or data "hostage" until money is paid, are delivered via phishing attack where people are tricked into providing sensitive information. With phishing being the most popular types of attack, training is paramount.

1 Evans, Gregory D. (2018, March 19). Cyber #attacks are one of the #biggeset #threats that #schools face, experts #warn. Retrieved from **https://nationalcybersecurity.com/cyber-attacks-are-one-of-the-biggest-threats-that-schools-face-experts-warn/** .

Attacks and Resolution

Different types of incidents require different response strategies. Most attacks fall within four general categories. Below are those four categories as well as possible steps to minimize the risk of the attack and contain the attack after it has occurred. Please note this list is not exhaustive.

TYPE OF ATTACK	PREVENTION/CONTAINMENT/REMEDIATION
Interception Attack-unauthorized access to confidential information, similar to eavesdropping or wiretapping *Examples:* man-in-the-middle attack, evil twin attack, packet sniffing, keylogging	• Block all unnecessary ports at the firewall and host • Utilize IP address filtering/blocking • Block entire countries or locations if there isn't a legitimate need for access • Limit the ability for infrastructure to communicate with the internet
Interruption Attack-a network resource unavailable for use. *Examples:* DoS or ransomware attacks	• Work with Internet service providers to block access further upstream • Implement automated tools to prevent overloaded traffic/ throttle traffic • Protect endpoints • Filter out spam emails • Block malicious links and IP addresses • Block all unnecessary ports at the firewall and host
Modification Attack-unauthorized modification of assets *Examples:* altering programs so that they perform differently, reconfiguring system hardware or network topologies	• Utilize Secure Sockets Layer (SSL) certificates, data encryption, and secured (WPA) wireless networks
Fabrication Attack- counterfeit message in the system *Examples:* insert messages into the network using identity of another individual, spoofing a website or other network service	• Utilize SSL certificates and data encryption • Filter incoming and outgoing traffic • Enforce account lockout for end-user accounts after a certain number of attempts • Follow the principle of least privilege

Cyber Incident: malicious event that compromises or disrupts, or attempts to compromise or disrupt, a cyber asset or its operation

Denial of Service (DoS) Attack: when an attacker attempts to prevent legitimate users from accessing information or services by flooding the network with information.

Evil Twin Attack: counterfeit wifi access point established to eavesdrop on wireless communications

Malware: malicious software designed to harm computers and computer systems

Man-in-the-Middle Attack: when the attacker intercepts a conversation to eavesdrop or to alter the communication.

Packet Sniffing: a form of "wiretapping" where a "sniffer" is used to intercept network packets, or data.

Phishing: when an email recipient is tricked into providing sensitive information.

Ransomware: software designed to hold a computer's functionality and/or data "hostage" until money is paid.

Reporting and Notification

When an incident occurs, reporting of the event to authorities and notification to individuals whose information has been compromised is often needed.

Federal Requirements

The Department of Homeland Security (DHS) collects attack information such as phishing email messages and website locations to help others avoid becoming victims. Additionally, they perform analysis on malware and other vulnerabilities to provide actionable information on how to better protect data systems. DHS keeps the information on specific victim confidential unless permission is received to release that information. Please see the links below to report incidents to DHS.

- **Report a cyber incident**
- **Report a phishing incident**
- Report Malware and vulnerabilities to DHS by emailing **cert@cert.org**.

State Requirements

In the event of a breach, an incident in which personal information is viewed or stolen, Louisiana law requires notification of the breach to the impacted individuals (note that there are currently no federal requirements.) Louisiana legislation requires entities to notify Louisiana resident,s without unreasonable delay, of any data breach that results or could result in unauthorized acquisition of their unencrypted personal information. Notification is not required if an investigation determines that there is no reasonable likelihood that the affected individuals will be caused harm by the information's loss. Breached entities that fail to notify the Attorney General within 10 days of notifying affected individuals may be fined up to $5,000 per violation. (**LA RS 51:3071** and **LAC Title 16, Part III, Chapter 7, Section 701**)

Helpful Links:

- **Incident Notification Toolkit**
- **Framework for Improving Critical Infrastructure Cybersecurity** by National Institute of Standards and Technology (NIST)
- **Computer Security Incident Handling Guide** by NIST
- **CIS Critical Security Controls for Effective Cyber Defense** by the Center for Internet Security (CIS)
- **Guide to Malware Incident Prevention and Handling for Desktops and Laptops** by NIST
- **Guide to Integrating Forensic Techniques into Incident Response** by NIST.
- **Cybersecurity Assessment Tool (CAT):** Electronic tool that helps establish school's current risk profile.
- **Stop.Think.Connect by DHS:** a campaign to increase the public's understanding of cyber threats and empower them to be safer and more secure online. DHS's **toolkit** provides tips and flyers that can be used when talking to students and to staff.

STEP 6: INVOLVE PARENTS

Based on the 2015 Future of Privacy Forum as communicated in the **2016 Forum Guide to Education Data Privacy**, parents support the use of student data at the local school for educational purposes. However, the use of data by third parties is a common concern specifically, advertising or marketing, the release of sensitive data, and identity theft. Therefore, it is critical to involve parents in data governance planning. Communication and transparency are critical for parents to feel comfortable with sharing their child's information.

***COSN** provides infographics (ready-to-go and customizable) to assist in communicating with parents and community members.*

Parental consent and notification of rights are both incorporated in almost all student privacy laws, for example, CIPA, COPPA, and FERPA. As part of a strong data governance action plan, LEAs and schools should make parent notification available at all times on their website and at their central office.

*Sample notification language can be found in **Appendix B**.*

Additionally, LEAs and schools should present this notification to parents annually for review. LEAs may choose to do this in their yearly Student/Parent Handbook, in a beginning of the year newsletter, at an open house, or at an in-person parent meeting.

Put Into Action

Parental Notification	Conduct an annual notification period where parents are notified of • **Parental rights under FERPA and PPRA**, • Any collection of information under specified events as outlined in **PPRA**, • **The adopted school board privacy policy**, and • The opportunity to not participate (or participate) in information being shared via school directory, online services, surveys, screenings, or marketing.
Parental Consent	Collect **parental consent** for • Any online services that collect student information for instructional purposes (**COPPA**), • LOSFA and BOR (**LA R.S. 17:3914**), and • Any other applicable programs where student information is shared (**LA R.S. 17:3914**).

APPENDICES

APPENDIX A – TERMS TO KNOW

- **Aggregate Data** are statistics and other information that relate to broad classes, groups, or categories of information.
- **Directory Information** is defined by FERPA as "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed." Directory information can be disclosed provided public notice of the specific elements declared as "directory information" has been made and parents have been provided the opportunity to opt out of the disclosure. The directory information exception allows students names and statistics to be released publicly for sports events, honor roll, playbills, yearbook, etc.

SPECIFIC TO LOUISIANA: Louisiana: R.S. 17:3914 requires parents to provide **explicit consent** rather than **implied consent** for the release of directory information. This means parents must be notified and written parental consent must be provided before their child's information can be shared. The process for directory information moves:

- **From Implied Consent:** Notify parents and allow time for them to sign a notification that they do not want their child's information shared.
- **To Explicit Consent:** Notify parents and wait for them to sign consent for their child's information to be share

---

However, 17:3914 (H) permits school boards to establish a policy that would allow a person employed in a public school or other person authorized by the superintendent of the public school or school system to be provided or having access to a student's records. Some LEAs and schools have relied on 17:3914 (H) to adopt policies that allow directory information to be shared unless a parent opts out as per FERPA.

- **Data Sharing Agreement** is an agreement between an educational institution and a third party, usually a contractor. The agreement defines the rights and responsibilities of each party regarding the confidentiality of, access to, use of, and dissemination of student data.

SPECIFIC TO LOUISIANA: R.S. 17:3914 specifically requires that data sharing agreements have both security audit and data breach language.

- **Disclosur**e is to permit access to, release, transfer, or otherwise communicate personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.
- **Disclosure Avoidance** are efforts made to reduce the risk of unintentional disclosure, such as applying statistical methods to protect PII in aggregate data tables. These safeguards can take many forms (e.g., data suppression, rounding, recoding, etc.).
- **Parental Consent** refers to consent or permission given on behalf of a minor child for data to be shared. **Consent can be explicit** where information WILL NOT be shared unless action is taken by the parent, or **consent can be implied** where information WILL be shared unless action is taken by the parent. A **conservative approach** would be to collect a consent that provides parents either opportunity in the same document. LEAs must collect and maintain these consent forms; they are valid in perpetuity unless the parent revokes his or her previous consent with another written document.
- **Personally Identifiable Information (PII)** is often defined slightly differently in each privacy law but includes direct PII as well as indirect PII. Generally speaking direct PII can be defined as the student's name, the name of the student's parent, guardian or other family member, the address of the student or student's family, a personal identifier such as the state student identifier or social security number. Indirect PII consists of personal characteristics and other information that when combined would make the student's identity traceable.
- **School Official** is someone that has a legitimate educational interest and must review the education record to fulfill his or her professional responsibility such as a teacher or principal. FERPA does not specifically define school official but does require that each LEA or school do so in their annual parent notification.

APPENDIX B – LAWS IN MORE DETAIL

THE CHILDREN'S INTERNET PROTECTION ACT (CIPA)

The Children's Internet Protection Act (CIPA) is a federal law that applies to LEAs and schools that receive discounted telecommunications, such as Internet access, under the Federal Communications Commission's E-Rate program. CIPA requires that LEAs have an Internet safety policy and technology to block access to obscene or harmful content. LEAs must also monitor their students' online activities and educate them on appropriate online behavior.

The Internet safety "policy must address the following five components:

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

"Prior to adoption, CIPA requires reasonable public notice and at least one public hearing or meeting be held to address the proposed Internet Safety Policy." Most Internet Safety Policies are folded into an LEA's acceptable use policy for students.

Sample language:

E-Rate Central's Sample CIPA-Compliant Internet Safety Policy

Ascension Parish School Board (pg 50)

THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

The Children's Online Privacy Protection Act (COPPA) is a federal law governed by the Federal Trade Commission (FTC). COPPA assures that children under 13 years of age do not share personal information on the Internet without the express approval of their parents.

Providers must obtain consent from parents to collect information, unless they are collecting on behalf of the LEA or school and will only use the information to provide services to the LEA or school. If this is the case, then the provider can rely on consent obtained from the LEA or school. LEAs can consent on behalf of a parent for educational purposes.

COPPA defines personal information as:

- "A first and last name
- A home or other physical address including street name and name of a city or town
- Online contact information as defined in this section
- A screen or user name where it functions in the same manner as online contact information, as defined in this section
- A telephone number
- A social security number
- A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier
- A photograph, video, or audio file where such file contains a child's image or voice
- Geolocation information sufficient to identify street name and name of a city or town
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above."

FTC-Recommended Best Practices

- Allow parents to review the personal information collected.
- Ensure operators delete a student's personal information once the information is no longer needed for its educational purpose.
- Notify parents about the websites and online services to which it has provided consent on behalf of the parent concerning student data collection, as well as the operators' direct notices. This information or a link to this information can be maintained on the LEA website.

SPECIFIC TO LOUISIANA: R.S. 17:3914 limits the sharing of student PII. When using online services without a data sharing agreement or parental consent, PII cannot be utilized.

Text of FTC Rule

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a federal law that that affords parents the right to have access to their children's education records, to seek to have the records amended, and to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student.

Generally, written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows records to be disclosed without consent under the following conditions:

- School officials with legitimate educational interest
- 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
- State and local authorities, within a juvenile justice system, pursuant to specific state law.

Some LEAs and schools have relied on 17:3914 (H) to adopt **policies** that allow directory information to be shared unless a parent opts out as per FERPA.

FERPA Regulations

Sample Notification

Directory Notification Sample

PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA)

PPRA is a federal law designed to protect the privacy of students in the administration of surveys, medical exams, and marketing.

PPRA restricts the non-educational uses of student data by requiring explicit parental consent before students can participate in any kind of government-funded survey, analysis, or evaluation covering particularly sensitive topics below.

5. "Political affiliations or beliefs of the student or the student's parent
6. Mental or psychological problems of the student or the student's family
7. Sex behavior or attitudes
8. Illegal, anti-social, self-incriminating, or demeaning behavior
9. Critical appraisals of other individuals with whom respondents have close family relationships
10. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers
11. Religious practices, affiliations, or beliefs of the student or student's parent
12. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program)."

PPRA states that there are three types of notification an LEA must provide parents and students.

1. General notification of their rights under PPRA
2. Notification of specific events.
    e. "The administration of any survey containing one or more of the eight protected areas listed above if it is not funded in whole or in part with Department funds
    f. Activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes or otherwise providing it to others for that purpose
    g. Any nonemergency, invasive physical examination or screening that is: (1) required as a condition of attendance; (2) administered by the school and scheduled by the school in advance; and (3) not necessary to protect the immediate health and safety of the student, or of other students"
3. Notification of the policies LEAs are required to develop, in consultation with parents, under PPRA. The LEA shall provide the notice at least annually, at the beginning of the school year, and within a reasonable period of time after any substantive change in the policies.

Under the PPRA, personal information is defined as "individually identifiable information including:

- A student's or parent's first and last name
- A home or other physical address (including a street name and name of a city or town)
- A telephone number
- A social security number"

Sample Notification

LOUISIANA'S STUDENT PRIVACY LAW (R.S. 17:3914)

R.S. 17:3914 is a Louisiana law designed to protect the privacy of students. It provides limitations and prohibitions on the collection and sharing of student information.

Prohibitions:

1. LEAs cannot require the collection of non-academic data about students such as political affiliation or religious practices.
2. LEAs cannot share personally identifiable information about students with external entities unless the data sharing meets one of the law's limited exceptions.
    a. The parent has given written consent to share that information.
    b. A person authorized by the state to audit processes, including student enrollment counts.
    c. The LEA has contract for student and other education services that include specific terms outlined in the law.
    d. An individual has been authorized by the Superintendent to perform specific duties for purposes outline in school board policy

Requirements:

1. Unique student identifiers
    a. The Louisiana Department of Education must create a system of unique student identification numbers. Students must retain their unique identifier throughout their tenure in Louisiana public schools. LEAs must assign and maintain the unique student identification numbers.
2. LEAs must gather parental consent for sharing PII with the Louisiana Office of Student Financial Assistance and postsecondary institutions through Board of Regents for purposes of financial aid and college admission.
3. Data sharing agreements must contain language that addresses how data will be protected including security audit and data breach language.

Consequences

Unlawful disclosure of personally identifiable student information is punishable by a fine of not more than ten thousand dollars or imprisonment for not more than three years, or both.

School Board Policy

R.S. 17:3914 (H) allows for local public schools boards to adopt policy that determines what data can be provided or accessed to perform specific duties. LEAs should work with local stakeholders and counsel to enact this policy. It is important to note that local school board policy cannot contravene federal policy and should be consistent with previous definitions of directory information.

Many are using a local school board policy to address common school-based processes that require data sharing like posting student information in school buildings, hiring school photographers, and printing graduation programs.

Sample School Board Policy from St. Tammany's School Board (Pages 6-10).

R.S. 17:3913

R.S. 17:3913 is a Louisiana law designed to provide transparency around data sharing.

It requires that LDOE provide the following information about the transfer of personally identifiable information available on its website and requires that LEAs make this information available at the main office of the governing authority.

1. A copy of the signed agreement
2. A complete listing of data elements
3. The purpose for sharing
4. The name and contact information of the primary point of contact
5. A process for parents to register a complaint

R.S. 17:112

R.S. 17:112 is a Louisiana law provides for the transfer of students' academic records. Each local education agency must provide education records within ten days of receiving written request from an authorized person on behalf of an educational entity where the student is enrolled or seeking enrollment.

The entity may be located within Louisiana or outside of Louisiana and may be:

- A public school
- A nonpublic school
- An education facility within a correctional
- An education facility within health facility

The record must include dates of any suspensions and/or expulsions, if applicable. The record cannot be withheld due to fine, debt or obligation.