

Data Privacy/Cybersecurity

2019-2020

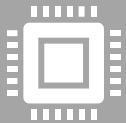
How do we ensure
protection of
student and staff
data?



What is Cybersecurity?



The protection of Internet-connected systems and data from accidental damage, intentional attacks, or unauthorized access.



Systems include networks, servers, computers and other hardware and software.



Data includes user-generated content and personally identifiable information.

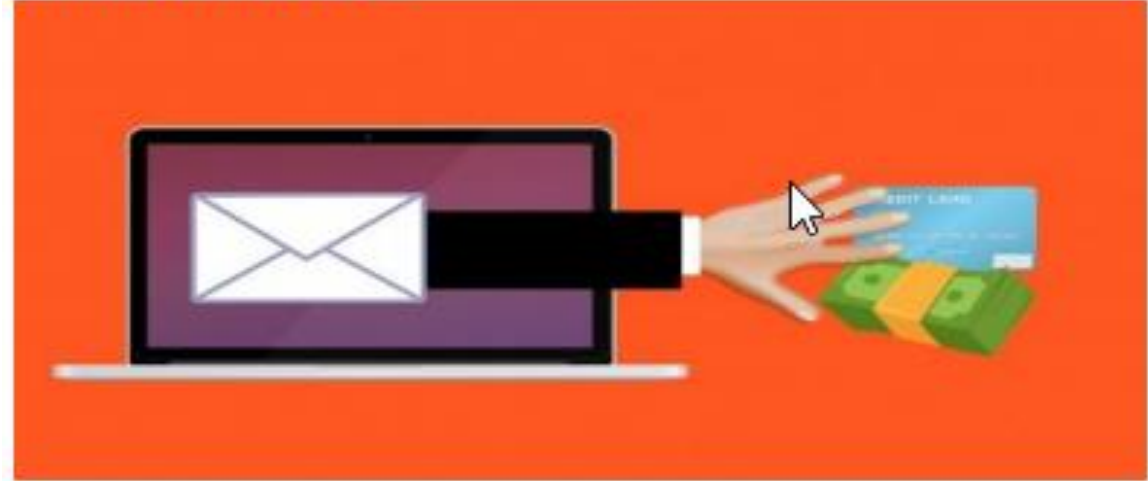
What is Data Privacy?

- How an organization determines the authorized access of the data it stores to be shared with third parties.
- How an organization complies with the legal requirements of how it handles information.



Why focus on Cybersecurity and Data Privacy Now?

Ransomware



Education Law 2-D



What is Ransomware?



- A type of malware virus that encrypts computer systems and locks user files illegally.
- It is usually delivered via malicious Web ads or via spam scams that trick users into clicking an illegitimate email file attachment or link.
- Ransom payments are demanded in order to regain access with a decryption key

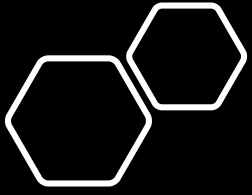
Ransomware in the News



Rockville Centre pays almost \$100G to hackers after ransomware attack, officials say



Newsday: Rockville Centre pays almost \$100G to hackers after ransomware attack, officials say



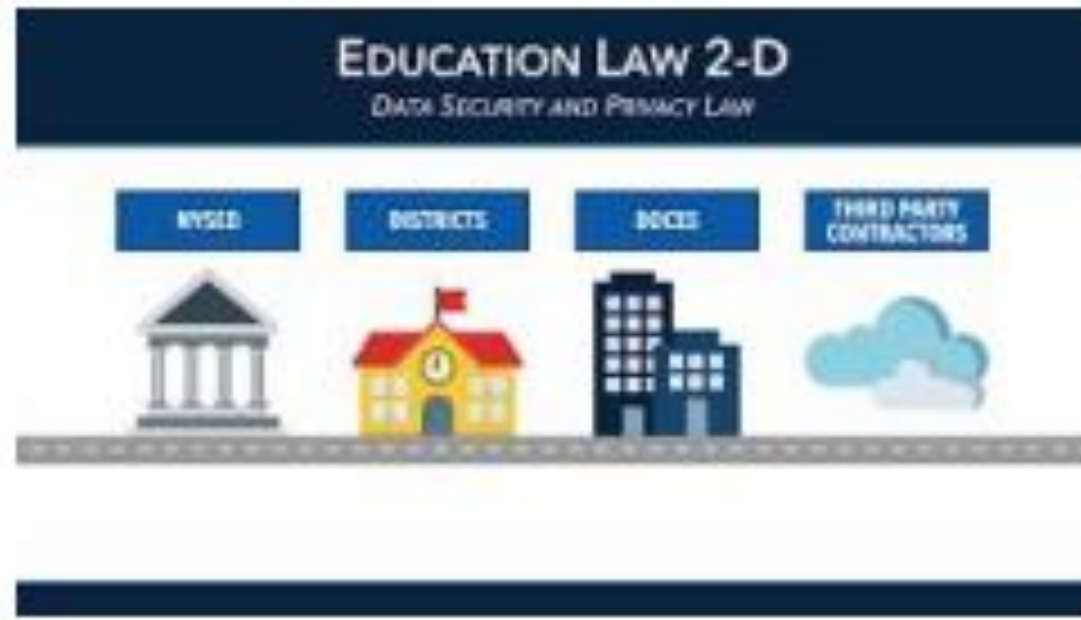
Ransomware Statistics

- Over 500 US schools were hit with ransomware in 2019. *
- Map of U.S. Ransomware Attacks.
 - U.S. medical, educational, and governmental organizations.



Source: Armor Cybersecurity, September 26, 2019

Source: PC Matic Antivirus, October 15, 2019



What Is Ed. Law § 2-d?

- Went Into Effect in April 2014.
- Prohibits the unauthorized release of personally identifiable student, teacher, or administrator data.
- Requires Parents' Bill of Rights for Data Privacy and Security.
- Requires Software Supplement.
- Requires both of the above to be posted on school district websites.
- Implementation regulations have been under development since then but have not yet been approved and released by NYSED.

Parents' Bill of Rights for Data Privacy and Security

Parents' Bill of Rights:

- To inform parents of the legal requirements regarding privacy, security and use of student data.
- Parents' Bill of Rights, with software used, must be posted on website
 - Due diligence must be made to ensure all online tools/software is in compliance with Law 2d.

Law 2d:

- To foster privacy and security of Personal Identifiable Information of students and staff
- Ensures data safety when...
 - Sharing student data, using software and online tools

What is PII?

- FERPA protects personally identifiable information (**PII**) contained in student records:

- Students name
- Parents name
- Physical address
- Social security number
- Date/Place of birth
- Mother's maiden name
 - Alone or in combination

Personal
Identifiable
Information



Understanding Data

- **Personally identifiable** information refers to any information that could identify the students. 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.

Technology Empowers

**Power of
Technology
allows us to.....**

**Meaningful
Technology
integration in the
Classroom**

**Anytime, Anywhere
Learning**

**Collaboration between
Students**

“With Great Power Comes Great Responsibility”

Taken from Eileen Belastook “Data Privacy: Are We Keeping Ourselves and Our Students Safe” webinar

Power:

Meaningful
Technology
integration

Anytime, anywhere
learning

Collaboration between student & staff

Responsibility:

Instituting
Vetting Process
for App and
Software
purchases even
when using
outside funding

Providing Data
Privacy Education to
Teachers, Staff, and
Students

- Developing Responsible Use Guidelines
- Digital Citizenship
- Creating a new school culture

Modified from [Student Data Privacy Communications](#)

Federal Student Privacy Laws

- **FERPA:** Family Educational Rights and Privacy Act
- **NSLA:** National School Lunch Act
- **IDEA:** Individuals with Disabilities Act
- **PPRA:** Protection of Pupil Rights Amendment
- **COPPA:** Children's Online Privacy Protection Act



These laws are designed to protect student data and prohibit any misuse.

Protecting Student/Staff Privacy



When choosing Software, keep in mind:

- Do students/teachers need to add any **PII** information?
- How does the Software vendor **PROTECT** student/teacher data? (Are they protecting their data or sharing their information?)
- At the expiration of the agreement, how do they **DISPOSE** of student/teacher information?
- Where is the student/teacher data stored- **LOCATION**? What are the security protections they are taking to ensure data is protected.
- **Purpose** for data collection?

Note: All software requests should go to your supervising AP.

All approved software must be put in Parent's Bill of Rights

Communicating via E-Mail

BOCES
DEPARTMENT OF REGIONAL SCHOOLS AND INSTRUCTIONAL PROGRAMS

Protecting a File with Encryption/Password

1. Begin your new document or Excel file
2. From File menu select "Info" > "Protect Document/Workbook"



3. Select "Encrypt with Password"
4. Enter a secure password, click on OK. Re-enter password again, click on OK.

Note: if you forget your password, it CANNOT be recovered.

5. Save file to desired location
6. Attach the protected file via E-Mail. Share the password with the recipient over the phone or in person.




Keep your data safe!

BOCES Department of Regional Schools and Instructional Programs | 110000 Road, P.O. Box 9775, Dallas City, TX 75209-0775
972.969.6000 • Fax: 972.969.6000 • www.bocesdallas.org

- Strong password – combination of letters and numbers
- Be aware of sender. Report suspicious email
- Office 365 to Share Files
- Email – Password Protect Files with PII information; call sender with password.

Communicating via E-Mail

	To:...	hdiamond@anyschool.org
Send	Subject	Ezra Stand

Dear Principal Diamond,

Please come to a parent conference for senior Ezra Stand next Friday at 3:00PM. Ezra has been absent from my class nine times this quarter, and even when he is in class, he is entirely disrespectful and verbally abusive to other students. I know his emotional disturbance is a factor, but there must be something that can be done to bring more order to the classroom. Ezra has a failing grade for this marking period, and there's no chance that he will be able to pass this course this year.

Thanks,
Diana Dion

PASSWORDS ARE LIKE TOOTH BRUSHES



Passwords...

Keep them private, make
them strong,
Never SHARE

Resources



[Student Data Privacy
Communication Toolkit](#)



[Online Training Videos](#)



[US Department of Education
Protecting Student Privacy](#)