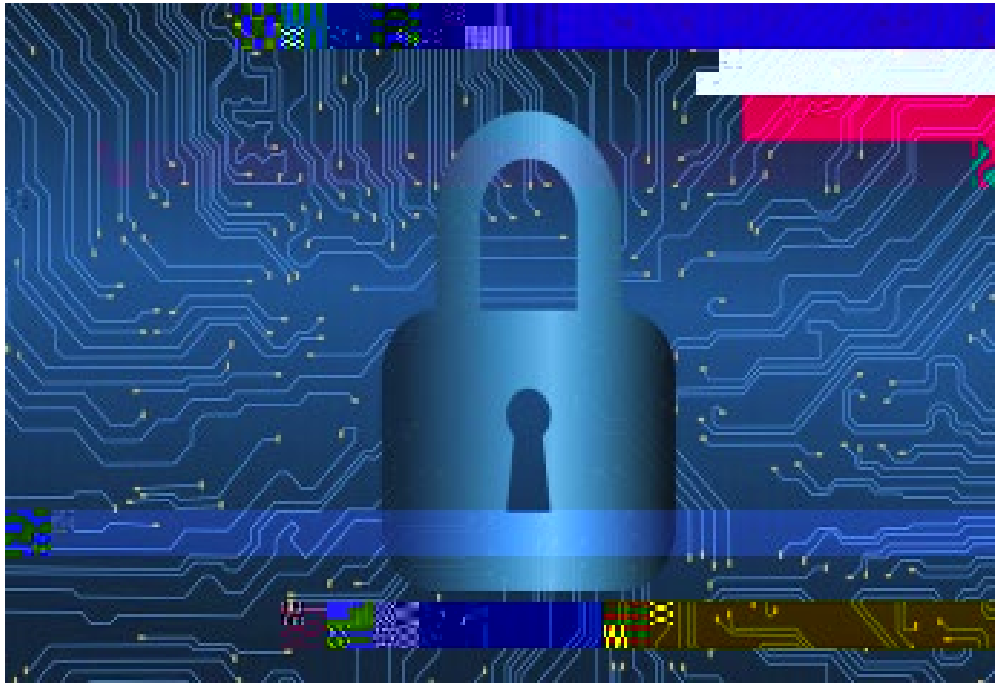
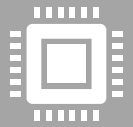
Data Privacy/Cybersecurity

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.



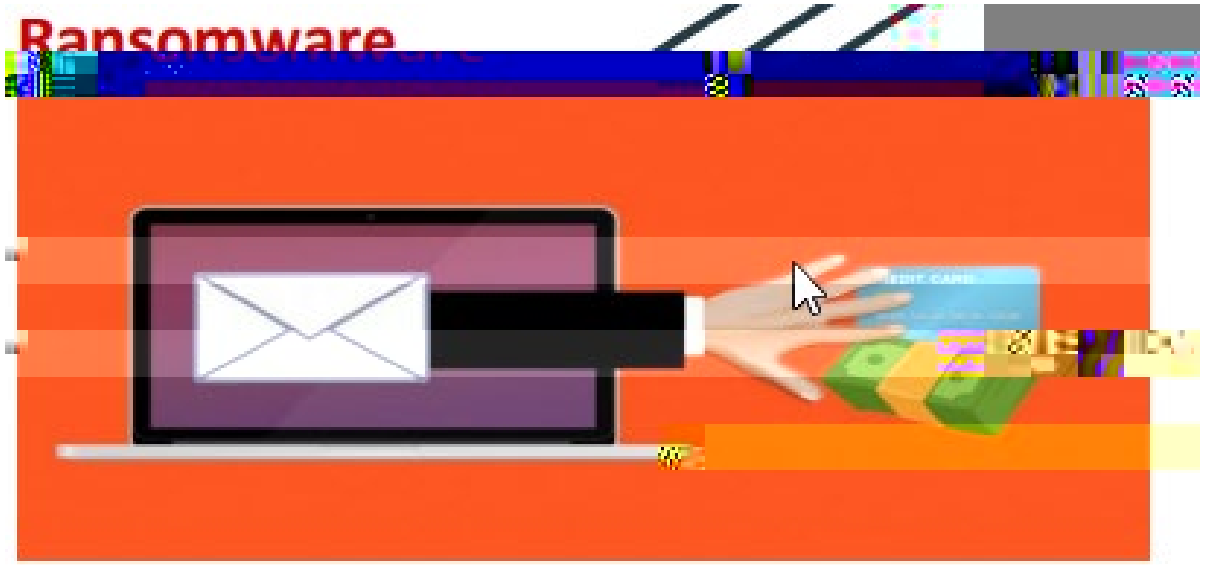
-

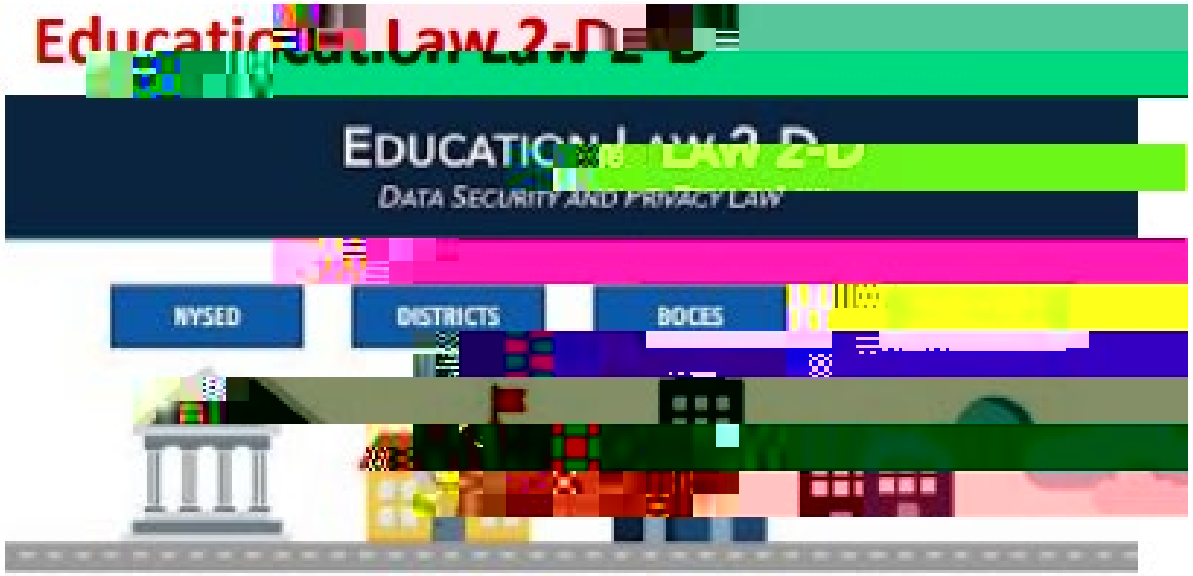
What is Data Privacy?

- 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?



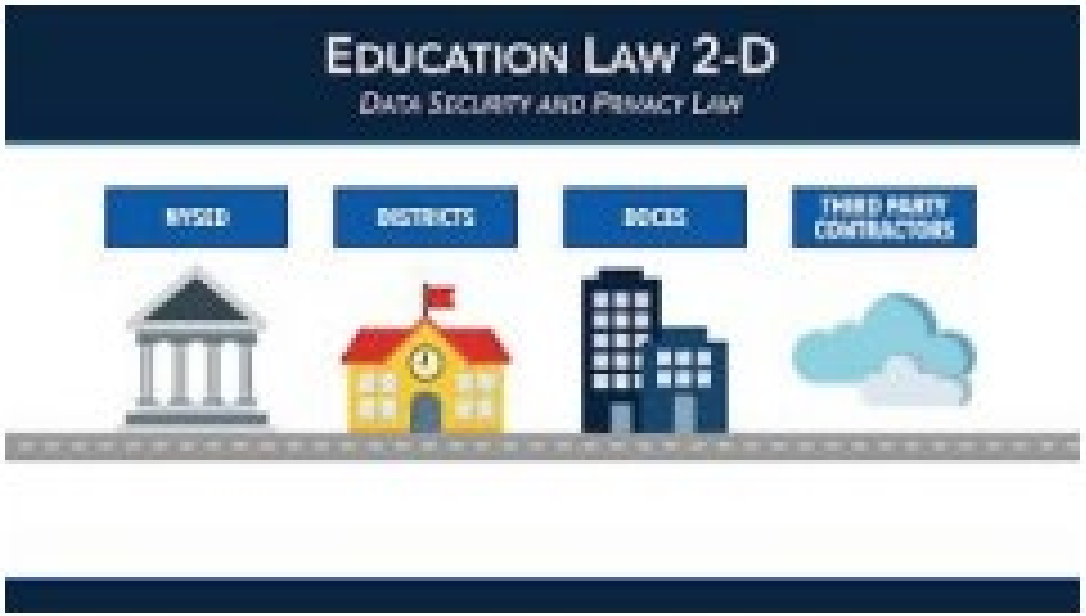


~Some information shared by Great Neck Public Schools

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

~Some information shared by Great Neck Public Schools



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

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:

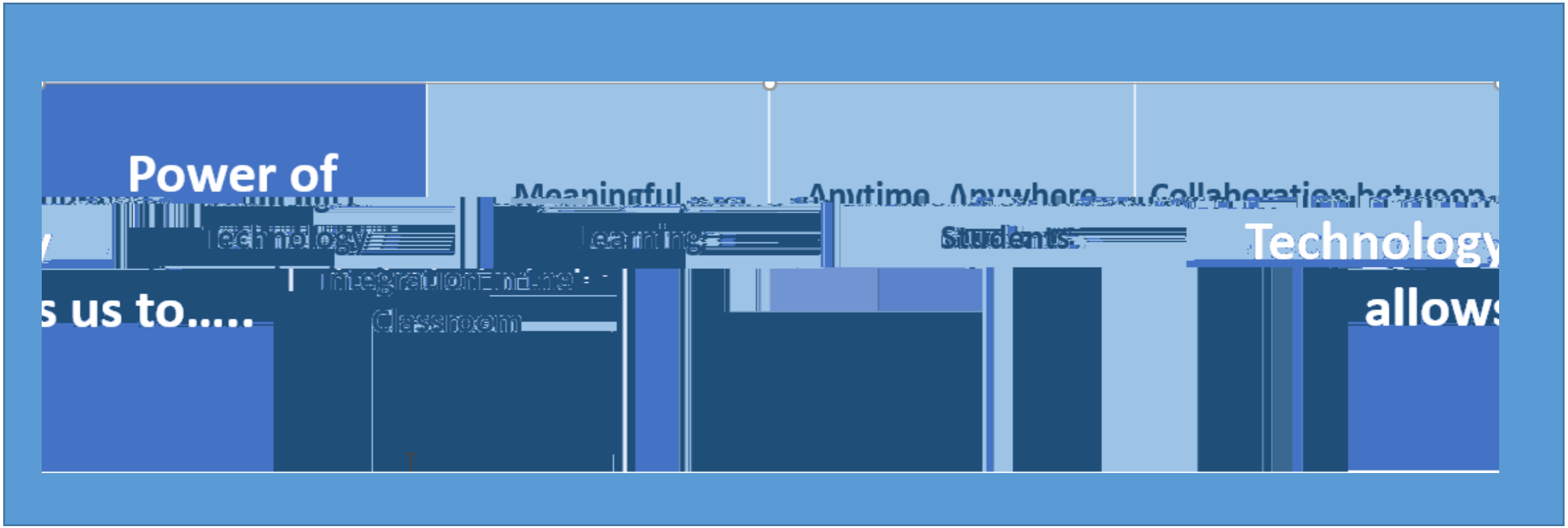
- To fodtcurit6 (r)-0.6 .7(w)9.1 ()-3.7(c)-3.8(y)3.3 (,)-0.9 7ndrDatsu tt dat136 -7(.)]TJ

What is PII?

-

Understanding

Technology Empowers



Modified from Student Data Privacy Communications

“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**			

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.

Modified from Student Data Privacy Communications

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?

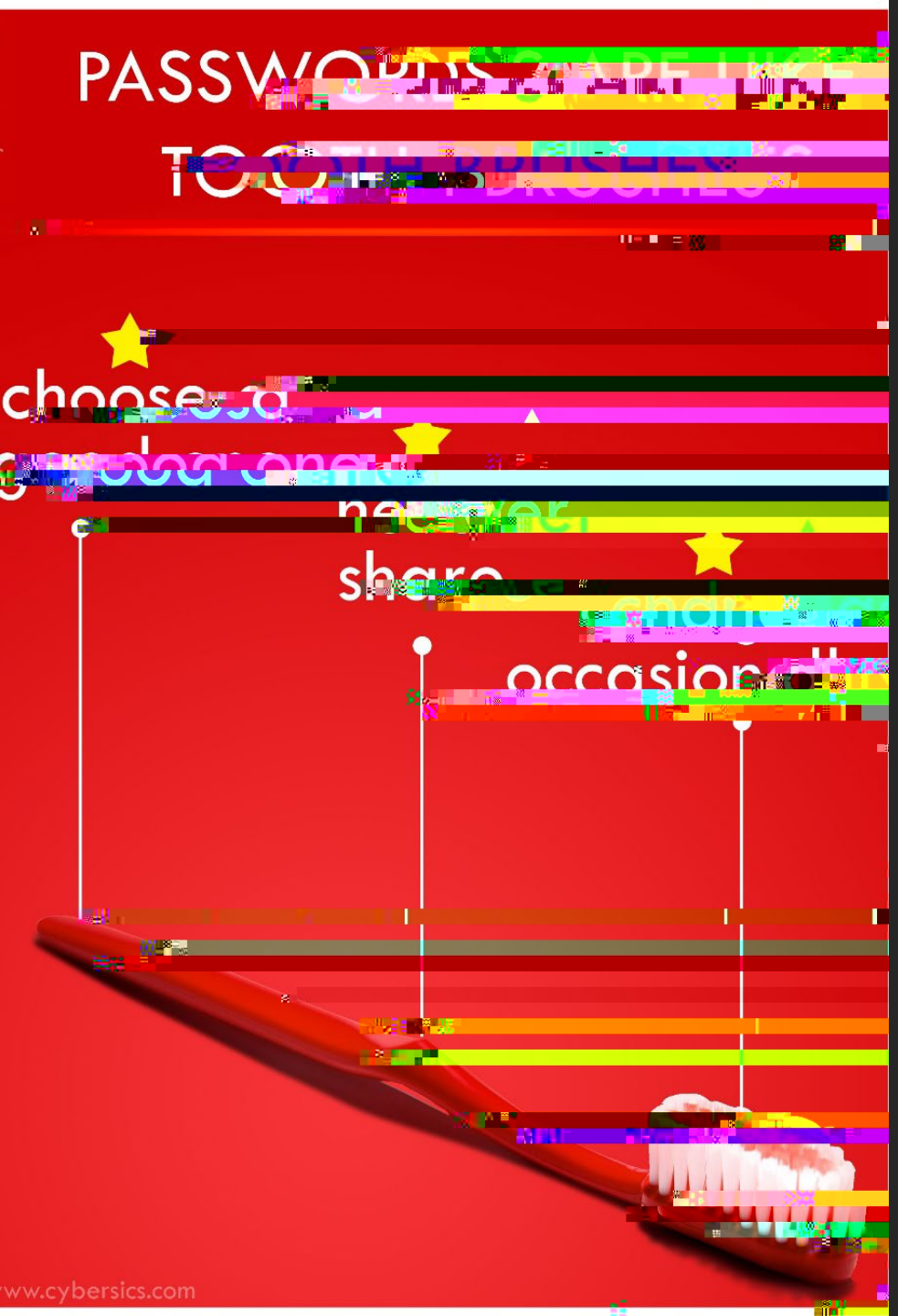
Note: All software requests should go to your supervising AP.

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

Communicating via E-Mail

- 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

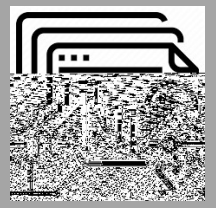


Passwords...

Keep them private, make them strong,
Never <u>SHARE</u>

Resources

Student Data Privacy Communication Toolkit



Online Training Videos

US Department of Education Protecting Student Privacy