Best practice recommendations for protecting district data

DPSS Spring User Group 2019

May 10, 2019

Step 1

DON'T PANIC!!!!

Step 2

Inventory all software applications used within your district. This includes both paid and free products used by students and staff.

Step 3

Review all software applications for both federal and state data privacy and security compliance.

REVIEW

Step 4

Determine if all software applications meet the district's data privacy and security standards.

STANDARDS

Step 5

Retire legacy software products that impede network security upgrades.

RETIRE

RIC one DPSS

Step 6

Post the district Bill of Rights Supplemental Page, along with district Parents' Bill of Rights document, for parents to access

NYSED Parents' Bill of Rights

Nassau BOCES Parents' Bill of Rights

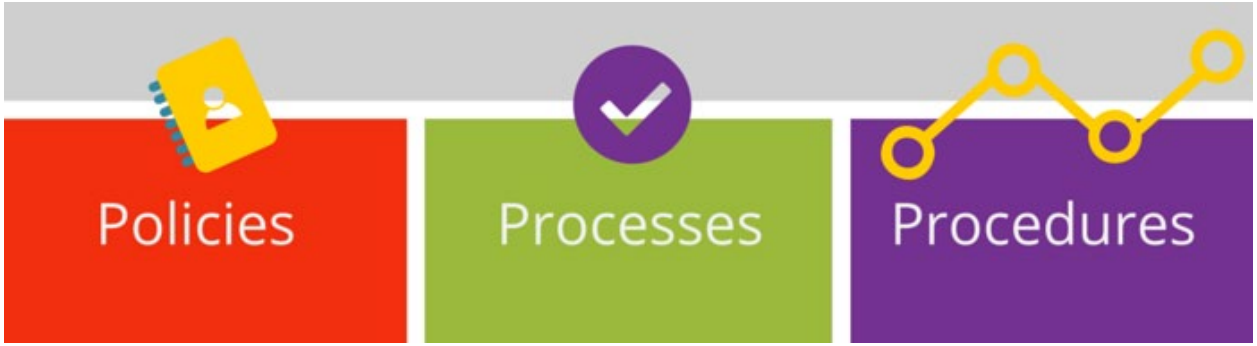
POST

nassau BOCES

Step 7

REVIEW, ADAPT, ADOPT district data privacy and security policies. Some example policies include:

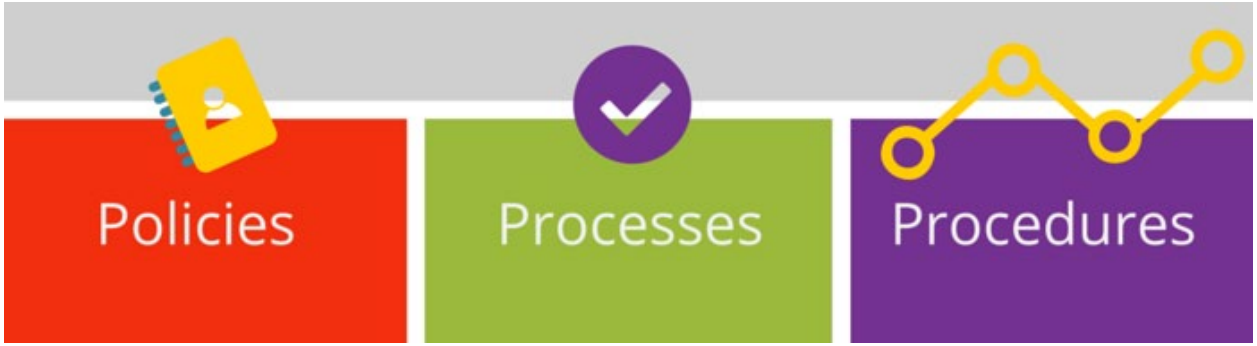
- Software application adoption policy
- Data breach and recovery policy



Step 8

REVIEW, ADAPT, ADOPT district data privacy and security procedures.

- For requesting software applications and edtech
- What to do in the event of a data breach
- How to process parent complaints



RIC one DPSS

Step 9

Deliver cybersecurity training to ALL STAFF and STUDENTS.

TRAIN

nassau BOCES

Step 10

Take a deep breath and continue these practices throughout the year, every year.