

Developing an Internal Vetting Process

Goal:

The district has a National Data Privacy Agreement (NDPA) for every resource that has access to student Personally Identifiable Information (PII).

Assemble a software vetting team with these roles:



Privacy



Budgetary



Technical



Curriculum

Create an inventory of software applications



Prioritize resources to pursue NDPA



Sensitivity of
data



Scope of
use



Upcoming
renewals



New
purchases
(RFP+NDPA)



Pilot
programs

Ask if use of the software application aligns with the district's educational goals and policies.

Review how the data is collected and used



Solely for
educational purposes



If used for commercial purposes,
parental consent may be required

Determine if a NDPA is necessary

If any of these are yes, a NDPA is highly recommended.

- ☐ Is student PII being shared with a third-party?
- ☐ Does the application collect student data (PII)?
- ☐ Does the student need to create an account and click a box to agree to Terms of Service?
- ☐ Will the student produce content in the platform or be scored/evaluated within the platform?
- ☐ Does the data create an educational record?
- ☐ Can the student interact with others on the platform?
- ☐ Do the Terms of Service have an age requirement that your students do not meet?
- ☐ AI – If the software application uses artificial intelligence (AI), determine whether the AI system is open or closed. If open, parental consent may be required. If closed, pursue a NDPA.

Next Steps



Include this in your Student
Data Privacy Program



Create a request process
for future requests