

To protect student data and ensure secure implementation, all software, platforms, applications, websites, and other digital resources that collect, store, access, or share student data must be reviewed through the district's Digital Content Procurement Process before use. This requirement applies to all resources, including free, purchased, grant-funded, donated, new, and renewal products.

New Purchases Or Renewals:

1. **Evaluate the Resource:** When selecting digital content/resource/program/software, it is recommended that your team utilize the [NC Digital Learning Initiative: Quality Review Tool for Digital Learning Resources](#) to help ensure that the product meets the school's needs and serves as the best option.

Additionally, schools are encouraged to use the **1EdTech Dashboard** to review a product's current status and whether it has previously been reviewed or approved by the district. Reviewing this information before submitting a procurement request can help schools make informed decisions and streamline the approval process.

1EdTech Dashboard Link: <https://app.1edtech.org/embeddable/trustedApps/1047>

2. **Submit a Digital Content Procurement Request:** Prior to purchasing, renewing, or using any digital resource that will access or receive student data, submit a Digital Content Procurement Request through the Droplet platform. The request must be approved by the principal or department head before implementation. This requirement applies to all resources that access student data, including free applications, subscriptions, purchased software, grant-funded resources, and donations.

Droplet Digital Content Procurement Form: <https://app.droplet.io/form/01kZZN>

Purchases with 418 and 411 object code must have the completed approved form uploaded to LINQ. The principal/department head's approval is required. *Any licenses or subscriptions purchased by CTE with the 411 object code will also need to be reviewed and approved prior to purchasing.*

3. **Vendor Documentation (When Student Data is Shared):** If the resource will collect, store, access, or receive student data and has NOT already been approved on the dashboard, the vendor must provide the documentation required by NCDPI. Documentation will be uploaded to the Droplet form. The following language may be shared directly with vendors:

Please send in the following documentation. For more information, vendors may access additional details at www.dpi.nc.gov/about-dpi/technology-services/third-party-data-integration.

- ☐ [Completed the 3rd Party Vendor Integration Worksheet](#)
- ☐ Completed [Data Confidentiality and Security Agreement for Online Service Providers and Public School Units](#)
- ☐ Completed Vendor Assessment Tool: [NCDIT Vendor Readiness Assessment Report \(VRAR\)](#), [Educause Higher Education Community Vendor Assessment Toolkit \(HECVAT\) Lite](#), [CoSN K-12 Community Vendor Assessment Toolkit \(K-12CVAT\)](#), or 1EdTech Security Rubric (pending public release)
- ☐ Completed FedRAMP, SOC2 Type 2 audit, ISO 27001 certification, or HITRUST certification

4. **Purchasing (When Applicable):** If the resource requires a purchase, procurement approval must be completed before initiating the purchasing process. Once approved, the completed procurement documentation should be uploaded with the requisition in the LINQ Document Cabinet as required. An email will be sent to the submitter and bookkeeper upon final approval with the PDF attached. This

applies to purchases made using applicable object codes, including instructional software and CTE licenses or subscriptions.

5. **Implementation and Rostering:** Once purchases are complete, notify and include your school's STEAMA Digital Teaching & Learning Support Specialist on the enrollment emails and calls with the vendor to ensure proper rostering and setup.

After approval and completion of the purchase, if applicable, submit a 1:1 Plus work order ticket to complete the setup process so the Digital Teaching & Learning Specialist can assist in implementation. Early involvement ensures proper rostering, single sign-on (SSO), account provisioning, and technical setup for staff and students.