Summary of the May 2024 KY K-12 Education Technology Leaders' Virtual Meeting

In case you missed it or want a refresher, the following is what we talked about during the May 20, 2024, EdTech leaders' virtual meeting. A copy of the video and audio can be found at: https://mediaportal.education.ky.gov/technology/2024/05/edtech-may-2024/.

Public viewing of the archived webcasts and written summaries are also available on the KDE Media Portal at: http://mediaportal.education.ky.gov/. Numbers in **RED** indicate the timestamp for that portion of the discussion so it can be easily located on the full digital recording.

This was a joint meeting with our OET staff and all the districts joining via Microsoft Teams and/or YouTube. We will continue to make these available from our KDE media portal so that you can watch the archived discussion and share with the appropriate people in your district. Several GoSoapBox poll questions were posed throughout the meeting and district EdTech leaders were asked to respond to all the questions as it assists us in planning and getting a feel for how to best move forward. Your voice and your feedback are important and extremely helpful to us. Please remember that in addition to these webcasts being available on the KDE Media Portal, each month's webcast is accompanied by these written summaries. We encourage you to share the link and all or any portion of these summary notes with staff throughout your district who may find the information beneficial to them in their position.

Before beginning with today's topics, David announced that Matt Jury has been named as the Division Director of School Technology Service and Chief Technology Officer (CTO) within the Office of Education Technology (OET). Matt is not new to our office and has served in several roles before accepting this new position. Matt began with OET in 2006 as a Team Lead. He moved into an Operations Manager role and then became Assistant Director within School Technology Services for six years. Most recently he has been the KETS Field Engineer in Region 7 for almost seven years. All of the candidates interviewed for this position were excellent, but we are lucky to have Matt in this role; he will continue with Region 7 coverage until his KE position is filled. Matt is the 3rd person to be the Director for this division. Phil Coleman recently retired from this position.

(7:09) KY K-12 CIO/EdTech Summit Follow-up – Topic #4 was on Cybersecurity and how to get people to care. We discussed this topic at our summit held in March at the Kentucky Society for Technology in Education's (KySTE) conference. Below is the "One Big Idea" table feedback for each of the 5 questions posed during the summit:

Q #1 - How do you get important cybersecurity communications to your Superintendent?

Bob highlighted some of major points/comments made by the tables during the Summit with one of the biggest items being having discussions face to face and developing a strong relationship between the CIO and the Superintendent; this will create the trust needed when there is a situation. Don't just focus on the Superintendent but also communicate and build relationships with the local board and local board attorney as well as the Chief Financial Officer (CFO). Bob encouraged everyone to read through all of the responses and realize how important this information can be.

Table #	The ONE Big Idea
Table 1	Starting with an e-mail so you have a paper trail. Face to face conversation is important to ensure that nothing gets lost in translation and to relay the importance of the topic. Put into the agenda of monthly staff meetings. Conversations with board members. Putting together a really slick and snazzy presentation to grab their attention. Attaching a message to a raven and sending it in the dark of night.
Table 2	Having a strong relationship with mutual trust. If something important comes up, text or go in and provide a recommended solution. Superintendent listens.
Table 3	Walk into their office. If it is something they absolutely need, follow up with an email so it is documented. A weekly conversation and the dialogue are already open with what is going on right now. Not fire hose them.
Table 4	Through face to face, attending administration meetings and sharing any incident to provide training on how it was a phish or issues; ask principals to reiterate the messages they are sharing with their teachers.

Table 5	Visual data, charts, internal phishing campaign with results provided to supervisors. Provide high level results to the Superintendent which generates discussion and opening for other cybersecurity topics/recommendations.
Table 6	In person with Superintendent, often in combination about costs (i.e., ransom), Bob's recommendation on best practices is in HIGH DEMAND
Table 7	If you're already having the conversations about tech (seat at the table) then you're already part of the story and including cybersecurity updates is just part of that. Also, it's really easy to say, "KDE is making us do this" and they just listen.
Table 8	Weekly district leadership meeting. Monthly/Annual cybersecurity updates at board meetings. Superintendent reaches out to the CIO requesting cybersecurity updates.
Table 9	Have a relationship with the superintendent to make the communications possible
Table 10	Face-to-face. However, there are times with providing the super with the monthly CIO agenda helps start a conversation.
Table 11	Use any opportunity to talk to them-if they're asking you questions about the insurance policy, use that time to talk to them about it. Email blasts.
Table 12	An email perhaps followed with a face-to-face "reminder". It's an occasional topic in a district admin meeting (if the CIO makes it a topic). When an issue is seen or addressed, email and follow-up discussions are still solid ways to get the word out. The email is still the intro and an excuse to have a deeper conversation.
Table 13	Regularly scheduled one on one mtg between CIO and Super.
Table 14	Meetings with super - one to one face to face discussions. Make sure district policies are followed. Regularly remind people of the district policies regarding security. Make sure school principals are involved and remind them regularly.
Table 15	Talk with superintendent concerning the risks. Share any updates as OET shares those updates. Speak at leadership meetings and do yearly beginning of year trainings
Table 16	CFO is leveraged since they have funds which are targeted by cyber issues. CFO then has conversations with the Superintendent who buys into the concerns for security issues.
Table 17	Email, call, face to face. Weekly cyber security questions through email with prices to get staff to participate. Train staff at the beginning of the year.
Table 18	Face to face, focused time and ask for BOE attorney (or SRO) to be present to team-up and make sure all are on the same page.
Table 19	Face-to-face then email to reiterate, bring data/reports to leadership.
Table 20	Weekly Core meetings, Scheduled face to face meetings, direct report meetings, trust relationship
Table 21	Including superintendent in CDW network audit and follow up conversations. As a result, the superintendent requested ongoing yearly audits. In person communication for important issues.

Q #2 - What's the best way to convince your district leadership to provide Technology (and cybersecurity) a permanent chair at the big table?

Don't spread FUD - Fear, Uncertainty, and Doubt. It's good to share stories/lessons learned from cybersecurity incidents as well as explaining the potential threats. It may also be "freaking out in a controlled way" and determining who in your district has influence. Many other things in a school are more evident of need, but we are beginning to be able to receive and share the data to help build that knowledge and trust.

Table #	The ONE Big Idea
Table 1	Let the superintendent know what exactly is at stake and what the fallout of something going wrong is going to be. Knowing the timing of what is going on and being strategic about when you approach the appropriate people for the ask. Don't be a "freaker outer" and come to the table with facts and information in a controlled way.
Table 2	Scare them enough by explaining the potential threats if something goes wrong. Explain that they must be involved in the selection of new products and services and the consequence if they aren't.

Table 3	The relationship building that goes with an earlier question allows you to be at the table. Conversations with other directors (including each other in the conversations). It's the small things coming out of a handful of teachers; not really an issue at the big table.
Table 4	Through sharing stories of breaches & incidents along with other issues and how it could impact our districts. Sharing with the Superintendent or Leaders on what we do have in-place and how we manage it to protect the district.
Table 5	State meeting with Superintendents to express cybersecurity issues, prevention, and need to support their local edtech staff in efforts to ensure a robust security program is in place within the district. This would help fortify reinforce/message from local edtech leader of consequences.
Table 6	Figuring out who is the heavy influencer (i.e., CFO), providing real life examples, Phishing campaigns,
Table 7	If they (district leadership) trust in your voice in all aspects of edtech then listening about cybersecurity is already part of the conversation. Getting a seat at the table and being a valued member of that "table" is vital… or nothing will work including cybersecurity issues.
Table 8	Money. Awareness- whether own attack or news of another attack keeping cybersecurity on leadership's radar. KY Homeland Security check
Table 9	Free or even paid reviews to showcase vulnerabilities in cybersecurity. Sometimes voicing or showcasing what would happen if we don't continue the service.
Table 10	Quantify the issue for them. Show how integral technology is to how we operate and how we educate.
Table 11	Fear-when it happens to someone else, you have their ear
Table 12	"Scare tactic" is a rough term but good to be informed and make leadership aware when an issue happens elsewhere, what it cost the impacted district, etc. Those stories will lead to regular updates being allowed in districts. Training for admins ad staff in general would help.
Table 13	Adding Cybersecurity as part of first of school list of training items, i.e., blood-borne pathogens, cybersecurity.
Table 14	Show them data. Let them know it is a real problem/concern.
Table 15	Share examples of other Kentucky districts who have had to deal with breaches, ransomware.
Table 16	Never let a good crisis go to waste. Use issues as a learning and jumping off point.
Table 17	Threat assessment and share findings with upper-level admin. Meet with IT staff on security and share meeting minutes with the board and superintendent.
Table 18	Fear. Real world examples. Loss of Money. Negative PR. Political issue.
Table 19	Share horror stories from other districts. Performed a phishing test within the district and presented results.
Table 20	Precedent, breach or attack to other district, awareness of educational targeting and 3rd party network security reporting.
Table 21	Proactive - Getting in front of issues with audits and continued communication. Show vulnerability on paper. Sharing cyber security issues in the news for awareness. Reactive - Embarrassment and cost after issues arise. This prompts a reaction.

Q #3 - Does cybersecurity need its own team in a district? Would a virtual or shared team be appropriate?

This one is challenging and sometimes we don't even know who or what we need to defend against. We need to try to figure out a way to have less dependence on KDE or one agency to help secure ourselves. Training is important and makes our jobs easier, but it has to be timely and meaningful. The idea of a shared/floating team was well received and we have to keep trying to find ways to do more with less. There could be many different versions of this "team". The collective thoughts on this one were very appreciated. We want to make sure, before we promote any free service(s), that it will work seamlessly in our environment and this sometimes takes time.

Table #	The ONE Big Idea
Table 1	Having a separate team would be nice but it's not a reality with the current funding that exists. It would be nice to possibly have a virtual or shared team that exists offsite or at a co-op that could be leveraged in the event that something happens.
Table 2	Internet security manager outside of the technology department. Meet as a team with technology staff once a month. Includes legal as needed. Even a larger district doesn't have the staff resources needed to be comfortable about cybersecurity. Prefer in district team.
Table 3	Trying to split some staff off for cybersecurity from security/content filtering. There are not enough resources or be able justify the position(s) in the small districts. Having guidance as to what works for one should work for most and would love for KDE to say you must do it this way (a standard vs your own team).
Table 4	Need a team, currently looking to provide training for district staff to get certified and assigned to cybersecurity. Vetting outside companies' offerings and looking at how to incorporate aspects of that work within the district.
Table 5	Would need enough depth and funding to run an entire team in the district. Could collaborate with other similarly sized districts to build team, likely virtual.
Table 6	Ideally have your own internal staff, shared Virtual from Co-op seems like a good idea if there are visible results
Table 7	Big district = yes, we have our own team. But it also needs to be somewhat independent of the other structures so they can make Smaller district = assigning different hats (multiple hats) to a handful of people. One person districts = wish I could have teams, not an option. A shared team model pushed out from the Regional teams we already have would be smart. Bring the resources to us in our teams that already exist.
Table 8	Cybersecurity is a hot topic and known area of growth. Wish there was a dedicated cybersecurity specialist. Partner with local cybersecurity group
Table 9	Yes. Virtual or shared team could work. Could see issues with partnering with other districts, especially if you are a large district. The amount of accounts and risk could monopolize the team which wouldn't be fair to partner districts. CUES should help with this (as a "shared model") for stale accounts. …we've been talking about CUES forever, but it should solve a lot of these problems for us.
Table 10	Possibly Co-ops or KETS regions get pen tests on a few districts and share results to create a line of best fit
Table 11	Could this be something Co-ops could provide if the staff needs help?
Table 12	Shared service was discussed, perhaps involving educational cooperatives. Some education/reminders would be needed with leadership to ensure that local CIO tech teams aren't "devalued" as a result of needing to outsource some help in this area. This might be a cybersecurity audit type of thing, PEN testing, etc.
Table 13	That specialized cybersecurity knowledge set is rare in school districts so a shared model would be the best.
Table 14	Maybe - depends on need and resources available IT touches everything from vendors to ops areas.
Table 15	Maybe - maybe DPP, HR, and Tech with superintendent to review and discuss processes and procedures.
Table 16	Two larger districts at the table saw "own team" as the approach while smaller districts realize it is a staffing and funding issue so it is shared. A virtual shared team could be the answer.
Table 17	Need a team but getting this to happen is going to be a challenge. Use outside resources to help address security issues in the absence of having a team. Think the idea of a virtual team by region might be more of a reality than a district team.
Table 18	Yes, a team or committee will create focus and not fall on just one person. Partnership with outside agency for yearly cybersecurity audit.
Table 19	Maybe. Depends on whether the appropriate members would show (Superintendent?)
Table 20	Virtual is cost effective, use of 3rd party detection, to identify areas for improvement.

Table 21	Districts in a regional area can form a cybersecurity team. A regional level team would be good for smaller districts. Data isn't going to reduce in size. Where are the cybersecurity jobs? Some students are interested in cyber security courses but what will they do with those? Yearly updates are a good time to touch base on cybersecurity.

Q #4 - Do you want/need a cybersecurity playbook and, if so, what does that mean to you? What are key features?

Responses were all over the place on this question with some of the more common responses being the most difficult to implement. We love the idea of a playbook but it is impossible to create the right level of detail for every situation; it could look like more of an incident response type of document.

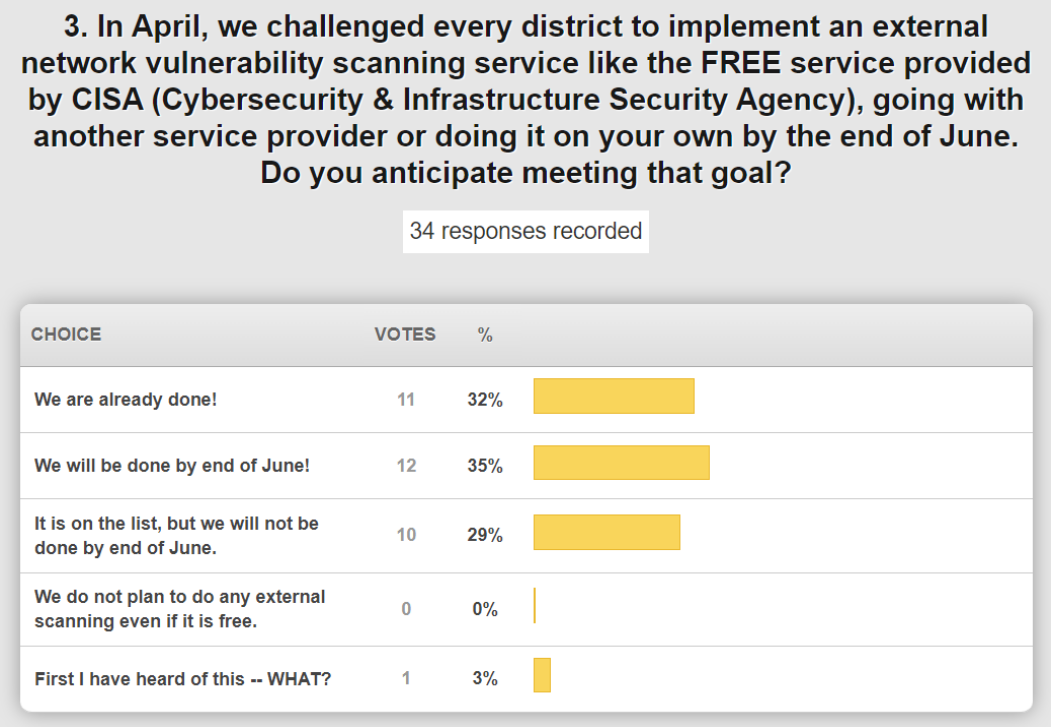
Table #	The ONE Big Idea
Table 1	A go to playbook, possibly month by month giving you ideas of the things that you need to be monitoring or reviewing to make sure you're on top of your cybersecurity settings. Would also be nice with a general layout of what KDE helps with or is responsible for versus what is the responsibility of the district. Could even be as granular as things teachers are responsible for, or helpful tips for them to improve their security.
Table 2	Send questions to an email group. Praise the person for sending as opposed to criticizing or shaming. Want a playbook. Working on one. It will be policies and procedures on what you can put on your device, security on your device, measures for a BYOD.
Table 3	You get hit with Ransomware; what do you do? Also, where do we start when we have a breach; what do we do to contain it? Quick response; don't send to the Helpdesk.
Table 4	We need a playbook and more guidance on various items. How to answer some of the insurance security questions and how to assist districts in incorporating some of the items required or needed for the insurance. What services and guidance can be provided or available for districts?
Table 5	Yes needed, should provide minimum best practices that districts could build upon. Should include training based on audience? Definition of current cybersecurity elements. Provide common scenarios and suggested remediation steps.
Table 6	Yes, need something specific for K-12, Free services, what to look for to stop breaches, tools (what Lewis Co uses)
Table 7	Need to be able to find anything we need in 3 clicks. When a breach happens, we don't' want to have to search through a 1000-page rulebook to find what to do. Accessibility to support is a big part. We need a simple KETS baseline for cybersecurity, then we can rely on KDE support to help dig deeper with guidance. We want a playbook with an exemplar to model. Steps 1, 2, 3 clearly stated by KDE on who does what, when they do it, how they record they did it, who they contact, and what they report to the people they contact. We're ready to be given the thou-shalls of cybersecurity from KDE/OET.
Table 8	Cybersecurity playbook for dummies. Step-by-step guidance. Who to call, when to call
Table 9	Playbook = good idea. Features could involve the breakdown of what's baked into the KETS environment for us versus decision points locally. Then what options are available/recommended, vendor relationship best practices or look-fors in this space
Table 10	Practices for new accounts and services. Get your 'Black Binder' for cyber response: Who to contact, first steps.
Table 11	Like this concept-Security Best Practices. Where can we get help-who will scan us, what can we do with the info afterwards?
Table 12	Playbook concept is solid. Stories of what has happened in KY K12, whether it's a data breach, security issue, a 'fix' applied somewhere. Something searchable would be preferred to "reams of information" in an email.
Table 13	Key Features: Best Practices for dealing with network equipment (baseline settings/configs), intentional time/day for cybersecurity,
Table 14	Yes, cannot tell you because it's a secret!!! Go to training - network CISA and other groups do not depend on Bob for all of your information -
Table 15	Yes, would be a great resource as districts do August updates and be mindful of some best practices.
Table 16	A Playbook would be best practices/audit of what needs to happen in the district. This might include an expert to assist.

Table 17	2-part playbook with preparation to be secure and the other part a break fix in the event something happens. Printable easily understood especially for new CIOs in case the district can't access the digital option.
Table 18	Yes, playbook with checklist of what to ensure is done for max security, OET recommendation for Cybersecurity, possible ranking of what is most important to have secure, recommend companies for internal audits, resources that can be shared directly with teachers and leadership, proactive elements to help prevent an attack
Table 19	Yes. The information that Bob presents (x number of phishing attempts in KETS, etc.). Info on exactly what to do if xxx happens.
Table 20	Security toolkit/response plan, identify vendors contacts, runbook for breach or attacks, and other cybersecurity related incidents and DR.
Table 21	It would be helpful. Steps to consider and what to do if you encounter a breech. More specifically on socially engineered attacks. Incident response plan and data on state incidents shared within the state.

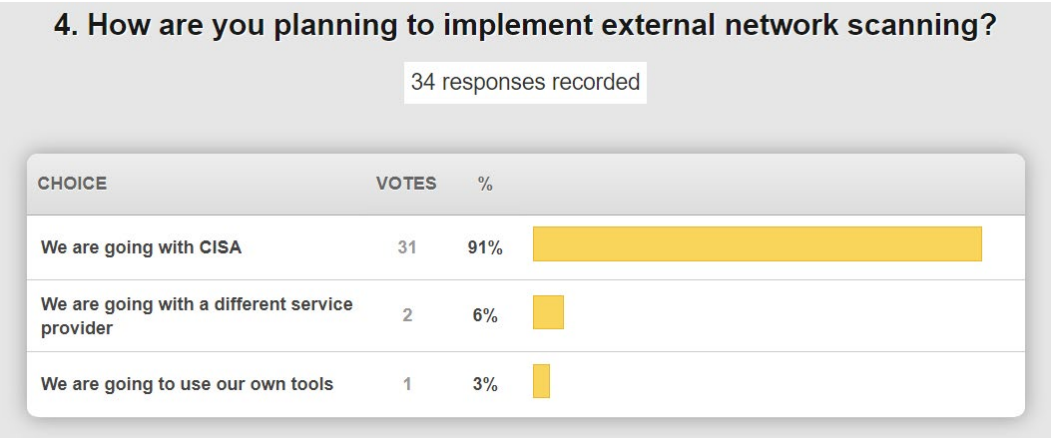
Q #5 - CISA provides a free service that will constantly scan external (internet-facing) services and devices via their IP address and send customized weekly reports to you. Is this something you would use, and will you sign up for this service by the end of May 2024?

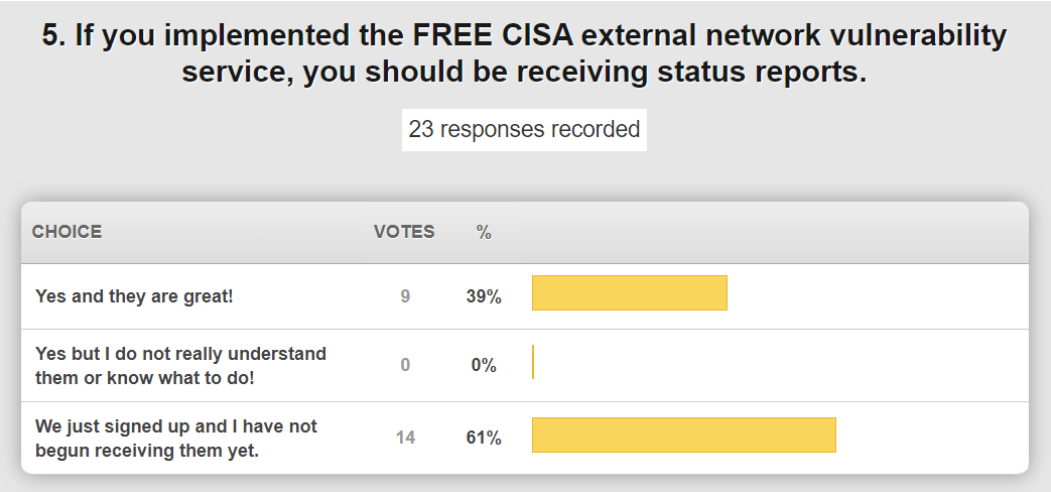
Table #	The ONE Big Idea
Table 1	Yes, districts will sign up as long as Bob agrees to sing.
Table 2	No one is using it. Some have been introduced to it. One is signed up. All will sign up. It may be 2-3 years if you sign up before its operational. If you're a district and don't use this, you're insane.
Table 3	Yes, everyone at the table wants to be signed up for the free service if they are not already.
Table 4	Yes, we will sign up. CISA will work with you to develop policies and guidance for your district. MS-ISAC is another free tool being used.
Table 5	1 worked with the help desk this week for scanning and testing, in less than 24 hours received listing of all public facing IPs. Others are interested in signing up.
Table 6	Yes. We used OET to help find external facing IP,
Table 7	We have a lot of questions about it, but it is interesting to those of us who have not seen it. The big idea at this table is this: we want KDE to roll out a large-scale, district by district, cybersecurity process with all of this included along with complete and customized guidance on how to make our district reach a best practice level of cybersecurity. Let's make Kentucky also be the national leader in cybersecurity in K-12. This should be just like all other OET roll outs of big edtech initiatives (ENA transitions, firewall, etc.). Please.
Table 8	100% plan on using if not already
Table 9	Yes, but May could be hard for some with all the end of year brings. Those that have started the process said there's information to supply and meetings to set up, which could be difficult right now. So, by end of June or July could work for sure.
Table 10	Yes.
Table 11	Yes. Some at the table have already used or are in the process of using this.
Table 12	All would sign up. There may be a wait list for some scanning services.
Table 13	Yes, some have already signed up. Some cyber insurance policies provide an hour of free service along these lines (vulnerability scanning).
Table 14	Yes
Table 15	Yes, include in August updates
Table 16	Yes.

Table 17	Everyone thinks this is a great idea and some are already working with CISA. Use the information with upper-level admin to educate them on what could happen.
Table 18	2 districts know about CISA, only 1 is aware of the services and plan to connect. All would like additional information.
Table 19	Yes. Some knew and some didn't. One is using.
Table 20	All members of this table have worked with, are interested or have scheduled a review with Colin.
Table 21	1 currently signed up to work with Colin. Yes, but help find the time to do it. Encourage superintendents to help make time for this. Regional expert from OET?



This is free and appears to be of high quality. We are excited to see these numbers and to see that almost 90% of respondents will have this done by the end of June.

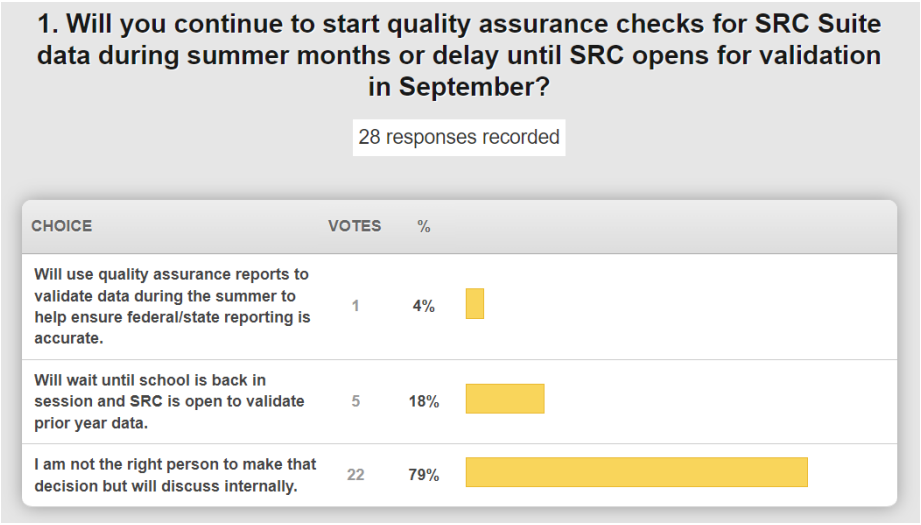




Everyone has received samples of these reports and we encourage you to take a look at those!

(42:39) Status of KY K-12 EdTech RFPs, Contracts and Implementations –

- **Next Generation KY K-12 Internet (NGKI)** – We continue to move forward and work is ongoing with ENA on a plan for any districts who have not transitioned by the end of the fiscal year.
- **Kentucky Educator Credentialling System (KECS)** – Continues to be implemented and there are a few more phases of that project.
- **School Report Card Suite (SRC)** – This has been awarded and that new contract continues to move forward with the selected vendor, Anlar. DeDe shared collection timelines for this year's data collection and also spoke to release of the dataset coming out separately from the charts/graphs views that will be later. The website address will be changing and the entire suite will be undergoing a rebranding.



- **Upcoming Contract Renewals** -
  - Instructional Device Contract – we are working to renew that contract while keeping the same status—you may use it but the requirement to utilize has been suspended
  - Network Device Contract – We are currently assessing those contracts and how we will move forward; this will need to be completed/in place well before the next E-rate filing window opens.
- **Insight** – The new contract holder as the Microsoft channel partner; this was effective in April 2024.
- The following items are currently in some stage of procurement process and moving forward:
  - KY K-12 Connected User Experience System (CUES)
  - Internet Content Management
  - Support for Education Excellence in Kentucky (SEEK)
  - Professional Learning Mgt System (PLMS) -This is for all adults that need professional learning that would be published or hosted by the Kentucky Department of Education.
  - Grant Management Application Planning (GMAP)
  - COT is establishing a new Microsoft Support Contract

(57:33) Updating and Modernizing OET's Portion of the KDE website - This has been in the top five feedback from our office staff and our districts and we are now focusing on this effort. A good first step has been made to make education technology more visible rather than be tucked under the District/School Support section of the KDE website homepage and we hope to make it even more prominent as we complete this work.

There are really three "What's" when looking at the OET landing page:

1. **What** are the key components that OET wants to market, highlight, educate and inform others about OET? The majority of this will be items from our 2024-2030 KETS Master Plan. (e.g., OET's areas of responsibilities, areas of emphasis, infographic, digital readiness, historic moments, budget, tech planning). Another item for consideration is the recent OET one-pager.
2. **What** content, beyond #1 above, is most requested and needed by our school districts (students, teachers, staff), KDE/OET staff, KETS partners, vendors, general public? We can get some of this from our website analytics and already know that eTranscripts is a big item. Another one is edtech contracts.
3. **What** are the items that OET points people to the most on the OET portion of the KDE website? In our discussions so far, we've identified the KETS Master Plan, KDE Media Portal, Infographic, KDE Digital Readiness, Open House, contracts, laws/regs.

Some cleanup efforts are already underway and are being done now before we make all the decisions on the future look/feel of our portion of the KDE website. We are looking at items on the current portion of the OET website that no longer serve a purpose and need removed/archived as well as items that need to remain but need to be updated/expanded to be most beneficial.

We reviewed the following GoSoapBox poll questions:

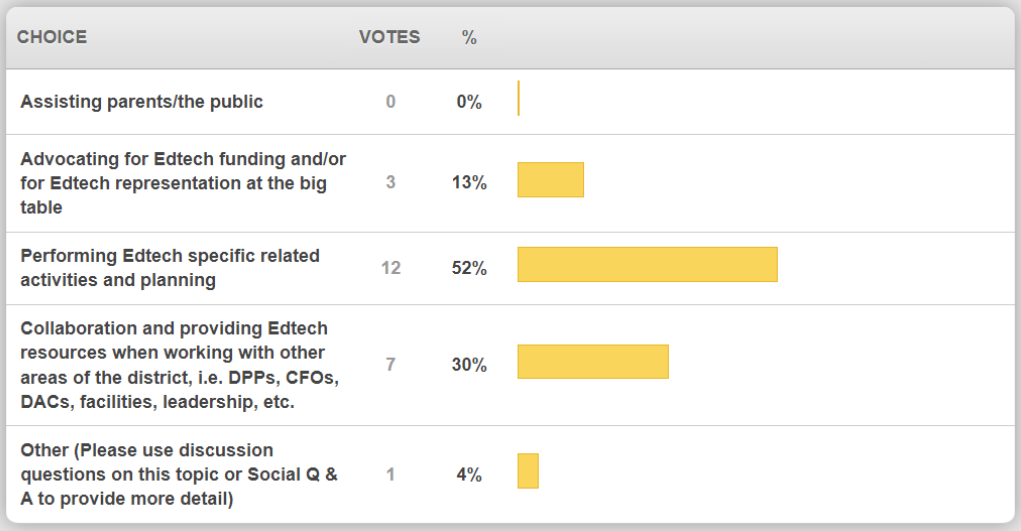
6. What aspect of the OET portion of the KDE website does your district find the most challenging?

25 responses recorded

CHOICE	VOTES	%
Navigation and/or Search	17	68%
Outdated Information	4	16%
Not enough relevant information	3	12%
Not enough detail provided	0	0%
Other (Please use discussion questions on this topic or Social Q & A to provide more detail)	1	4%

7. To better understand the information and/or resources most beneficial to districts going forward for inclusion on the OET portion of the KDE website, please select the highest priority use for your district of the site:

23 responses recorded

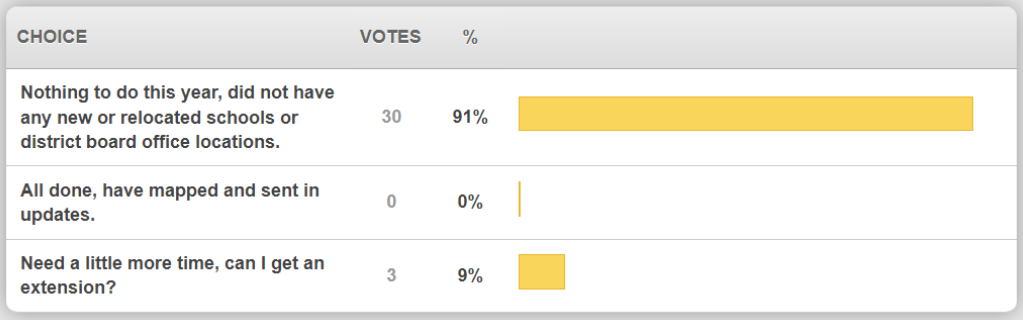


CHOICE	VOTES	%
Assisting parents/the public	0	0%
Advocating for Edtech funding and/or for Edtech representation at the big table	3	13%
Performing Edtech specific related activities and planning	12	52%
Collaboration and providing Edtech resources when working with other areas of the district, i.e. DPPs, CFOs, DACs, facilities, leadership, etc.	7	30%
Other (Please use discussion questions on this topic or Social Q & A to provide more detail)	1	4%

(1:05:14) Front Door Project Update – DeDe shared that we've received 20 updates and 9 photo updates for the mapping project. Changes are only made if your district has a add/move/change that needs to be made from the previous year's submission. We do have a few districts who requested a little extra time. If you have any questions about the Front Door Project—reach out to KDE data requests mailbox. The deadline was May 15th, but we'll assist in getting any final revisions completed.

2. Did you complete the Front Door initiative to report geographic coordinates for any new or relocated schools/district locations by May 15 or is more time needed?

33 responses recorded



CHOICE	VOTES	%
Nothing to do this year, did not have any new or relocated schools or district board office locations.	30	91%
All done, have mapped and sent in updates.	0	0%
Need a little more time, can I get an extension?	3	9%

(1:07:41) Affordable Connectivity Program (ACP) Update - We have been collecting connectivity beyond the school campus for close to 10 years now. This federal program ended at the end of April and David has been receiving calls and requests from media outlets. They are under the impression that we have a very large percentage of students without connectivity when in actuality it is only 2% and they are also unaware that Kentucky is/was the first state in having all schools connected. The impact of the ACP program going away is that K-12 parents are more likely to find a way to have connectivity in the home. Before the pandemic 95% of homes had enough connectivity with 2% not having enough and 3% being able to go somewhere nearby to gain access. After the pandemic we are at 95.5%. We won't see a significant and overwhelming impact on the

ending of this program; it was $30 per month or $360 per year. Continuing to make them aware of opportunities will be even more important. The federal Lifeline program still exists ($10/month) and many telco companies will also provide discounts. Helping our parents be aware and helping them through these discounts is a hurdle. Marty emphasized that our households in Kentucky were very far along and ACP provided for a .5% growth; this would have been normal growth for us regardless of the ACP program.

(1:15:37) Federal E-rate Audit Results Update - We have been undergoing an E-rate audit for funding year 2020; we received a little over $12M in E-rate rebates for that funding year on behalf of all school districts. Audits are normal and customary with any federal program, but this one was time consuming and resulted in no findings. We have not received the final, approved findings document but we expect that soon. Thanks to all the team members who were part of that.

(1:17:47) KY K-12 Online Testing Update - Paul Shoemaker is the Office of Education Technology liaison that works with the Office of Assessment and Accountability for online testing. Online testing is a team effort with the technology, our Internet service providers, OAA, and the testing provider—we do this very well and our success should not be taken lightly. The 2024 online testing is going very well and Paul thanked all of the district technology staff for their excellent work and collaboration with the District Accountability Coordinators (DACs) and Building Assessment Coordinators (BACs), preparing their schools for online testing, and making it a good experience for students. We are in the KSA testing window and have a few weeks left. At the time of the webcast, we had completed 1,577,000 successful tests. Peak day was May 8th with 242,606 tests completed.

(1:20:19) Healthy Data Diet of KY K-12 Social Security Numbers (SSNs) Update – We held a closed session/bonus time on the SSN topic after last month's webcast and since that time OET leadership met with KySTATS to discuss this topic. Matt Berry of KySTATS was very receptive and open-minded. Next steps will be meeting with leadership from KHEAA and KDE's Division of School and Community Nutrition. If we cannot eliminate them completely, can we reduce the collection to only include the specific grade level(s) needed. Using only the last four digits may be another viable alternative. Things have changed dramatically over the last 25 years and the current level of cyberattacks in the KY K-12 environment necessitates us continuing to advocate for change in the use and collection of SSNs.

(1:24:07) Other Items to Note:

- Federal ESSER Extension - OET leadership are working on items to submit for consideration in the ESSER liquidation extension application being prepared for all of KDE. If approval is received, it would extend the approved items until February 2026.
- EdTech Professional Learning Opportunities - Learning something new can be a form of recharging. Over the summer there will be multiple opportunities. Here are some of those:
  - Educational Cooperatives
  - Innovations for Learning Conference on June 4th (Fayette County)
  - Murray State Teaching and Learning Summit is June 11/12
  - Kentucky Reads to Succeed Conference is June 20
  - PBL Works
  - Castle Summer Refresher for Library Media
  - Teach Meets – happening statewide
  - KET Summer Learning Series
  - Infinite Campus Beginning of Year (BOY) Training is 7/18
  - Kentucky Digital Summit