Pennsylvania House of Representatives Education Committee
Public Hearing on Student Data Retention and Protection
Pennsylvania State Capitol
523 Irvis Office Building
Harrisburg, PA 17120
October 24, 2022

Written Testimony of
Danielle Mariano
Senior Vice President of Compliance, Commonwealth Charter Academy Charter School

Good morning, Chairman Sonney, Chairman Longietti, and honorable members of the House Education Committee.

My name is Danielle Mariano, senior vice president of compliance at Commonwealth Charter Academy Charter School.

Thank you for the opportunity to discuss the security of student information and how CCA ensures the protection of personally identifiable information from nefarious individuals and groups who wish to breach our networks and compromise the information of our students and their families.

CCA is the largest K through 12 public cyber charter school in Pennsylvania, with an enrollment of nearly 21,000 students from virtually every county throughout the state. As a student- and family-service organization with an expertise in education, CCA is focused on providing every student with a high-quality, flexible, customizable education that meets their needs and learning style.

In my role, I am focused on ensuring CCA remains in compliance with state and federal education laws and regulations.

I work closely with CCA staff, including the Technology Department, to ensure that student and family information is protected and only accessed by those who have job duties that require access to such information.

From the time student and family information enters our system at the application phase and throughout their time at CCA, it remains protected and secure.

Through numerous news reports, we have heard of various organizations, including schools, that have fallen victim to online attacks, hacking, and ransomware that have resulted in personal information being compromised and stolen and the loss of hundreds of millions of dollars. In some situations, organizations did not know of the attack until long after it happened.

Since this impacts every sector, schools have a responsibility to ensure their student information is secure and protected around the clock.

To ensure the security, protection, and integrity of student and family information, I will provide an overview of the measures CCA has put in place without revealing the specific details of the processes and systems.

As a K through 12 public cyber charter school, CCA is laser-focused on the protection and security of student and family information.

CCA's handling and protection of student and family information can be best described as an onion: student and family information is at the core, or center, and layer-after-layer of security features and systems protect unauthorized access.

Since we operate in the online environment, we take extra steps to and have systems in place that protect our students' and families' information. In fact, the measures and systems we have implemented are closely aligned with banking industry standards. CCA's network security currently meets the framework of the National Institute of Standards and Technology (NIST).

Through a dedicated technology team, comprised of credentialed industry experts, we have deployed enterprise-level security features that include multiple layers of firewalls, multi-factor authentication, advanced threat protection, virtual private networks (VPN), frequent and routine testing, and system redundancy.

Nearly one dozen staffers are dedicated to monitoring the activity of CCA's networks to ensure they remain secure and student information is protected.

We also work with third-party cybersecurity experts to stay apprised of current and potential vulnerabilities.

It is CCA's policy to house student and family information on physical servers in a secure location. Student and family data are not stored in any cloud-based systems. This ensures that personal information remains out of the hands of external parties and under the control of CCA.

In addition, CCA's learning management system – edio – and student information system – PowerSchool – are housed on physical servers under the exclusive control of CCA. It is our practice to not use web-based services to store student and family data.

While system security and protection are of paramount importance to CCA, it's also critical to focus on the human element.

Network security is only as good as the individuals who actively use and perform tasks on a day-to-day basis.

An area that is of utmost importance to CCA is educating employees since they are the first-line defense to preventing breaches of our network. All staff is routinely trained throughout the year to identify phishing scams, unauthentic email communications, and unsecure websites and internet links.

On a bi-weekly basis, our technology team deploys security tests to assess staff awareness and their ability to identify questionable activity and report it through the appropriate channels. Those who do not take the necessary actions are required to undergo additional training and demonstrate their understanding.

Staff is provided with computers that include enhanced and advanced technology to protect access to the information contained on their laptop as well as CCA's network. If connecting to our network offsite, staff computers are forced to operate through a virtual private network (VPN) regardless of where they are located. In addition, all staff is required to go through a multi-factor authentication process to log onto their computer and access our network.

Overall, CCA is ahead of the curve by using advanced security and protection measures for student and family information. Our state-of-the-art technology and equipment provide a multi-layered, multi-pronged approach to prevent unauthorized access.

CCA continues to review its policies, practices, and systems to further make improvements to tighten the security of our network.

Our goal is to assure our students and families that their information is secure and will not fall into the hands of unauthorized individuals.

Thank you for your time and the opportunity to testify before the committee.

I look forward to addressing any questions you may have.