PAcyber
The Pennsylvania Cyber Charter School

Main Office
652 Midland Avenue
Midland, PA 15059
p 724-643-1180
www.pacyber.org

Chairman Sonney, Democratic Chairman Longietti and members of the House Education Committee, on behalf of the Pennsylvania Cyber Charter School as well as the Pennsylvania Coalition for Public Charter Schools, I am Brian Hayden, CEO of PA Cyber. We welcome the opportunity to share the ways in which we protect all of our stored student data. Last year, after a local community college had a data breach, I asked our IT department if we were protected; their response was "as well as we can be". It was then that I began to understand the complexity of data protection and the changing and ongoing challenges schools are constantly adapting too. As discussed below, PA Cyber endeavors to take every precaution to protect its data and is constantly upgrading these processes.

What type(s) of student data does the school retain?
Required enrollment data and personally identifiable information (PII), educational records, special education records, and health records

Does the school retain parent/legal guardian data?
The school retains parent/legal guardian data required for enrollment purposes only. This could include proof of residency, name, address, phone, email address, custody agreements

How is the student data retained, and for how long is it retained?
Student data is retained according to the school's policies. The data can be retained in the form of physical records or electronic records. Electronic data is secured through user permissions. Physical student data is secured with restricted access in one of our office locations. Currently the school retains educational student transcript data for 100 years. Other student data is retained according to the school's policy and procedures.

How is student data secured, and how is it properly destroyed?
Student data is **secured** through a number of measures including the following:

- Internal controls that provide access only to employees that have reasonable and appropriate need for access.
- School policies for appropriate handling of student data
- System data and integrations are secured through encryption or tokenize
- Most student data is hosted on an internal network that is not publicly accessible via internet
- The school has network firewalls and application firewalls, Distributed Denial of Service Attack (DDoS) protection, content filtering, antivirus, and malware protection, endpoint management tools, and performs regular updates and backups.
- The school has contracted network infrastructure monitoring 24-7

Student data is **destroyed** in the following ways**:**

- System data is purged based on retention policy schedules
- Process of wiping and reimaging technology that is reused

- Technology hardware is recycled and destroyed by third party who issues certificates
- Document destruction is performed by a Secure Document Destruction Service

Does the school handle student data protection, retention, and safety in-house, or does the school contract with a third party?
The school manages student data protection, retention, and data safety both in-house and through third parties.

From where does the school receive guidance or training on student data protection, retention, and safety (if applicable)?
The school does regular research internally for industry standards and best practices. The school also often utilizes guidance from legal or third party managed service providers and consultants. The school also contracts with a third party to perform penetration testing to the school's network infrastructure.

What can the Legislature do to assist schools in terms of student data protection, retention, and safety?
It would be beneficial for the legislature to require the Pennsylvania Department of Education to provide more clear definitions and guidance for K-12 schools in this area. Including what student data is required to be retained and for what period of time. State or federal requirements for software application vendors to meet specific data security standards in order to contract with K-12 institutions. Additionally, a toolkit for K-12 would be a useful tool as well as funding and resources for training and professional development. Finally, enhancing resources to improve the marketplace for cyber insurance for schools. Currently, it can be difficult for K-12 schools to obtain cyber security insurance policies with adequate coverage or affordability. Additional education funding specifically designated for technology hardware and software would also be helpful.

Again, we thank you for the opportunity to testify before the committee and look forward to answering any questions you may have.