Office of the Chief Technology Officer

Student Data Privacy and Data Security Safeguards

Hardware

- **Firewalls/Content Filters**: MCPS utilizes numerous industry-standard safeguards for protecting students and student data from malicious websites, including:
    - Content filters: comprised of multiple platforms designed to protect student and employee from accessing inappropriate and explicit internet content, including malicious sites created to obtain personally-identifiable information from users
    - Firewalls: An appliance at the perimeter of our network designed to prevent unauthorized access to our network and keep intruders from using software to obtain student or employee data
- **Network Protections**: Follows network standards to limit network traffic safely through the use of VLANs to only allow guests and other non-MCPS users to access the internet and external traffic only, limiting any exposure to internal traffic and MCPS user data

Software

- **Permissions/Roles**: Access to user data for all MCPS-provided devices (servers, desktops, laptops, and mobile devices) is restricted to explicit permissions provided to each user through authentication
- **Antivirus/Antimalware**: All MCPS-provisioned devices are protected by antivirus and antimalware solutions
- **Operating-system Level Encryption**: All devices are protected with hardware-level encryption in case a device were stolen or otherwise compromised

Policy

- **Compliance Training**: Compliance training that all MCPS employees are required to take outlining the importance of student data privacy and the federal laws and best practices governing it
- **Guidelines**: General Use Guidelines, a document describing how to safely use new educational technology with student data, which has been developed in collaboration with instructional departments within the county, general counsel, outside counsel, and neighboring districts
- **Vetting Form**: An online digital tool approval form used by educators in the district wanting to receive guidance on how to safely use new platforms and software
- **Policy Changes**: Upcoming changes to Board Policy and Board Regulations outlining the requirement that all online digital tools must not only go through their original vetting process to be deemed instructionally relevant but must also be vetted through the aforementioned approval process and General Use Guidelines
- **Best Practices**: MCPS' Data Privacy Initiative complies with the U.S. Department of Education's best practices as it relates to student data privacy and FERPA compliance