Cybersecurity and Data Privacy: Kent School’s Response to the Clery Matter

Kent School is committed to running and maintaining an active cybersecurity and data privacy program, and we continue to strengthen that program as technology, threats, and best practices evolve. At the time of Daniel Clery’s wrongdoing, Kent already had important safeguards in place, including multi-factor authentication across the School community, separate privileged administrator accounts, endpoint security, controlled network access, and enterprise systems designed to provide appropriate roles and accountability.

Since we discovered Clery’s criminal conduct, Kent School has made significant investments and improvements in its technology and cybersecurity infrastructure. This work has included rebuilding our core virtualization environment, updating firewalls and network infrastructure, strengthening backup and recovery capabilities, expanding endpoint and email security, and engaging outside expertise to help manage and monitor critical systems.

A central part of this work has been increasing visibility, monitoring, and independent oversight. The School now maintains 24/7 managed detection and response, centralized security logging, network monitoring, vulnerability identification, and security operations support. Both Kent Technology and our managed service provider, Apex Technology Group, have visibility into security activity and alerts, providing additional checks and balances so that security events are not dependent upon a single individual for detection or response.

Kent has also strengthened identity and access controls. Separate privileged accounts remain a requirement for administrative work, multi-factor authentication protects administrative access, and certain high-level changes within systems, such as Google Workspace, require approval by more than one administrator. Tools now automate significant portions of account provisioning, role changes, and offboarding, helping ensure that access changes when an individual's responsibilities change. Access and permissions are reviewed periodically, and the School has completed reviews of shared-drive permissions and implemented a formal data-retention policy.

Protecting privacy also extends to how students and employees interact with technology. Student passwords remain the student's own, and when Technology staff need access to a student device for support, that work is performed transparently and with the student present. Remote-support sessions use an enterprise platform that provides logging and accountability. Kent's student bring your own device (BYOD) program does not require endpoint-monitoring software on students' personally owned devices; Instead, network-level security tools help identify threats and unauthorized activity while allowing students to retain control of their personal devices.

Kent regularly evaluates its security protocols through independent security and privacy assessments, vulnerability scanning, cyber-insurance reviews, and penetration testing, including an independent penetration test completed in spring 2026. Findings from these reviews help inform ongoing improvements and future investment.

The Technology team also remains actively engaged with professional organizations such as ATLIS, attends industry conferences, and consults with security partners and peer independent schools to evaluate emerging threats, share practices, and benchmark our approach.

Cybersecurity requires continuous attention as technology and threats evolve. Kent remains committed to a layered approach that combines strong identity controls, security technology, centralized monitoring and logging, tested backups, external expertise, transparent support practices, and regular independent review to protect the security and privacy of our students, employees, and School community.

Last Updated: August 2026