Kindergarten Through 12th Grade Security Information Exchange (K12 SIX)
K12 SIX is a cyber threat intelligence sharing hub for school districts, to aid in preventing and mitigating cyber threats. This non-profit member community is a cost-effective forum for crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security staff.

How It works
Each school district joins the SIX as a member, plugging its IT team into the community via a secure sharing portal. Through the portal, the district has access to actionable intelligence and alerts generated from data submitted by other members and multiple intelligence sources accessible to SIX staff. Peers in the community may contribute findings on specific malware, phishing attempts, and system vulnerabilities, and provide best practices and mitigation techniques. The K12 SIX staff provides in-depth threat analysis, facilitates collaboration, and integrates intelligence from partner security vendors, government sources, other sharing communities, and the Global Resilience Federation (GRF) international network of affiliates.

Common Threats to the Education System
Spear Phishing: An employee in Texas released the W-2 tax forms on all district employees to someone incorrectly believed to be the superintendent. Result: Widespread identity theft and tax fraud.

Ransomware: A Massachusetts school district fell victim to ransomware impacting its email, payment and web services. Result: Acting contrary to the advice of the FBI but in coordination with local law enforcement, the district paid $10,000 to restore access to its systems.

Poor Cyber Hygiene: An online Florida school had unencrypted, confidential student data taken and sold on the Dark Web. Result: More than 368,000 teachers, students and families had personal information accessible to threat actors.

DDoS: Multiple distributed denial-of-service attacks targeting the Central New York Regional Information Center caused connectivity issues. Result: The attacks impacted the ability to teach in dozens of school districts in central New York.

Insider Threats: A Chicago Public Schools employee stole personal information on her final day at the job. Result: Potential breach in the school system's database of 70,000 people, requiring public disclosure to meet data breach laws.

Institutional Knowledge
When Global Resilience Federation (GRF) creates a sharing community like K12 SIX, it works with the founding members to design a structure that meets their sector's needs. Intelligence is sourced specifically for the defensive requirements of that sector, with dedicated analysts who investigate and enrich member-shared information and external sources.

GRF excels at helping to build a *member-driven* community for stakeholders to connect, discuss, and support each other as they mutually enhance their resilience. K12 SIX analysts guide members, anonymize information, and enable control of how information is disseminated in the network.

GRF leverages 20 years of experience establishing, growing, and managing information sharing networks, and currently supports 10 different communities. Once a community is operational, GRF connects it into its cross-sector network of thousands of members, operating on five continents. In 2018, GRF-supported communities shared more than 4,000 intelligence alerts and reports, and millions of Indicators of Compromise.

Cynthia Camacho
VP of Community Development
ccamacho@grf.org
917-822-4067

Contact Cynthia with any questions about K12 SIX. The community is open to members and partners interested in funding, providing materials, security tools, or intelligence feeds. Learn more about GRF at www.GRF.org. Visit GRF on Twitter at @GRFederation or on LinkedIn at Global Resilience Federation.