Internet of Things/Smart Devices in KETS

What are Smart Devices and Internet of Things devices?

Devices that perform a service and connect to the local network, cellphone network, and/or Internet, but are not general-purpose computers or manageable mobile devices (smartphones/iPads).

These devices generally look like something we are used to interacting with physically or with some sort of dedicated wiring (e.g. speakers, HVAC systems, video surveillance), but now have embedded computers and network/wifi connections and make connections to apps or cloud-based services.

Examples:

Network-connected video cameras	Physical security monitoring systems (fire, intruder, breakage, flooding)
Voice over IP phones	Network Printers
Smart door locks	Intercom systems
GPS monitors on buses	HVAC monitoring/management systems
Smart speakers (Alexa etc.)	Elevators
Dedicated streaming devices (Roku, Chromecast, etc.)	Connected medical devices

What are the Risks?

As network-connected devices with computers inside them, these items have plenty of benefits, but come with their own risks, because their makers often prioritize speed to market and convenience over security and it is easy to ignore their potential for causing problems. In addition, there is little existing federal or state law to encourage makers to consider security and privacy.

Privacy Risks

- The vendor may intentionally use data collected by the device in a way that violates federal or state law or district privacy policies
- The vendor may not secure the device or the data it collects well enough to prevent data breaches or other security incidents

Physical Risks

- Malicious or curious persons may be able to take control of a device that controls a physical system (such as HVAC or door locks) and cause mischief or harm – such as raising the temperature of a school
- Malicious persons may be able to take control of a device with a camera or other sensors and use the information collected to plan mischief or harm against an individual or a building

Cybersecurity Risks

- Malicious persons may be able to take control of a device and use it for their own profit at a cost to the district – such as a distributed denial of service (DDOS) attack on an external site or cryptocurrency mining
- Malicious persons may be able to take control of a device and use it to attack other systems on same network, causing outages, data ransom or data breaches
- Devices may require network adjustments that increase the risk to other systems on network (require allowing certain protocols, etc.)

How do we minimize the risk?

Safer Procurement

- Look for well-known, trusted brands that will care about reputation versus simply the cheapest model from an unknown brand
- Look for enterprise-grade equipment over consumer-grade
- Look for privacy commitments from the vendor or manufacturer that address specific laws or regulations, preferably related to K12
- Look for support duration commitments – is any firmware current as of this year or last and how long/frequently will updates be provided? Can the vendor be trusted to keep that promise?
- Understand what data, if any, will need to be provided to the vendor/device on a regular basis and what data are automatically collected
- Require strong encryption during storage and over-network data transfer
- Look for central management capabilities, which will be more prevalent with enterprise-grade
- Determine what level of local effort will be required to implement and manage the device
- Look for the ability to reset to factory configuration & clear any data
- Clarify any ongoing support or operations costs (Total Cost of Ownership)

Safer Configuration

- Replace default passwords with long/strong passwords or passphrases
- Understand and consider the privacy implications (such as audio collected by Alexa-type devices)
- Configure device or system to minimize-required data collection
- Evaluate the risks and mitigations for each device or type of device (in the context of intended use)
- Configure centralized management and monitoring; reduce or prevent custom configurations
- Configure the minimum required services and network ports on each device (disable unnecessary services)
- Set up specific network filtering (at KEN district firewall if not internally) - in and out. Require VPN for remote management
- Consider placing devices in dedicated address ranges to simplify monitoring and security controls
- Consider placing devices in separate routed subnetwork traffic controls (similar to a DMZ)
- Configure access controls to allow the minimum needed permissions for each user or account

Safer Management

- Assign a specific team or person to oversee each type of device
- Update firmware/software regularly
- Maintain a central inventory of devices (requires managing acquisition/implementation)
- Periodically check for unauthorized physical connections (Ethernet, USB, SD Card)
- Periodically verify that all expected devices are still connecting to network
- Monitor network traffic for pattern changes
- Disable or remove unnecessary accounts

Safer Use

- Educate staff and students about IoT risks and how to safely use IoT devices
- Minimize unnecessary collection of sensitive data; i.e., turn off a smart speaker except when it is needed
- Remove collected sensitive data (such as video recordings) after a period of time appropriate to the purpose