Understanding Student Monitoring

Student monitoring programs are not new, but they have gained significant traction recently due to the increase in school-issued devices and the pandemic accelerated shift to remote learning. How do schools use these systems to monitor students, what data is collected, and how is student data used? Let's take a look:

WHY DO SCHOOLS MONITOR STUDENT DIGITAL ACTIVITIES?

Schools monitor students in an effort to preemptively detect threats to student safety and protect students, comply with state and federal regulations, and respond to community concerns.

SAFETY
To identify potential threats to school-wide and individual student safety, including content indicating violence, bullying, or an intention to self-harm.

COMPLIANCE
To control for potential compliance issues including monitoring and restricting students' access to content that may be inappropriate or harmful to minors.

COMMUNITY CONCERNS
To take a visible, active response to manage potential threats within their community, either due to prior incidents or as a way to demonstrate proactivity.

SCHOOL BOARD MEETING

WHAT TYPES OF STUDENT DATA ARE MONITORED?

Schools contract with third-party technology services that provide and manage student monitoring systems. School administrators interact with their chosen service provider to set up a monitoring system in a manner that meets their school's needs. Here's where the data is being monitored:
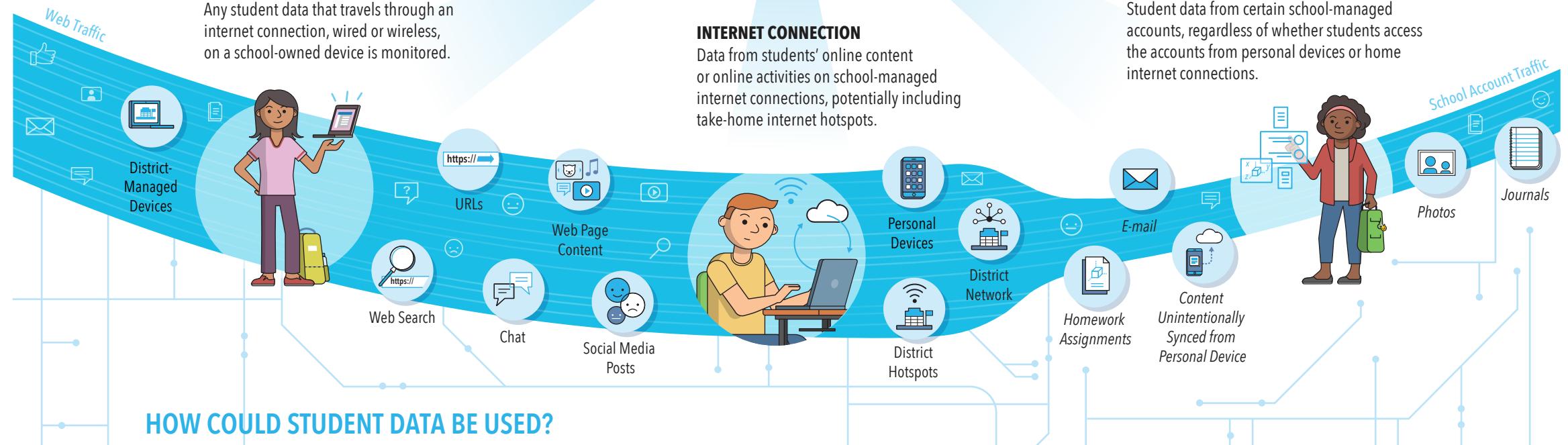
SCHOOL-ISSUED DEVICES
Any student data that travels through an internet connection, wired or wireless, on a school-owned device is monitored.

INTERNET CONNECTION
Data from students' online content or online activities on school-managed internet connections, potentially including take-home internet hotspots.

SCHOOL APPS & ACCOUNTS
Student data from certain school-managed accounts, regardless of whether students access the accounts from personal devices or home internet connections.

Web Traffic

District-Managed Devices

URLs

Web Page Content

Web Search

Chat

Social Media Posts

Personal Devices

District Network

District Hotspots

E-mail

Homework Assignments

Content Unintentionally Synced from Personal Device

School Account Traffic

Photos

Journals

HOW COULD STUDENT DATA BE USED?

ANALYSIS
The system analyzes the student data for potential concerning indicators, with some systems flagging content for human review. Indicators are typically related to potential self-harm, violence, bullying, vulgarity, pornography, or illegal behaviors.

ACTION MAY BE TAKEN
Depending on the nature and severity of the flagged content and product configuration, the following action(s) could be taken:

WARNING SENT

CONTENT BLOCKED

SCHOOL STAFF ALERTED
(could include school administrators, counselors, parents, or law enforcement depending on product configuration)

At any point in the process, student data may be saved by the school or monitoring provider either temporarily or long term.