Data Privacy and Security

This Photo by Unknown Author is licensed under CC BY-SA-NC

702 KAR 1:170

- Requires that the district acknowledge to its local board prior to August 31 of each year that it has reviewed the guidance of the KAR and implemented best practices

Relevant Board Policies & Procedures

- 01.61 – Records Management
- 01.61 AP.11 – Notice of Security Breach
- 09.14 – Student Records

Main Causes of Data Breaches

- Human Error
  - Accidental sharing (email, website, paper, etc.)
  - Weak or stolen passwords
  - Loss or theft of employee device (USB drive, laptop…)
  - Phishing, clickbait, ransomware

- Everything Else
  - Application vulnerabilities – unpatched software
  - Hackers
  - Malware

Security Breach Notification

Notify all individuals and agencies as outlined in KRS 61.933 if PII (Personally Identifying Information) has been disclosed and will result in the likelihood of harm to one or more persons

One of these

- First name or first initial and last name
- Personal mark
- Unique biometric print/image

AND

One or more of these

- Account number with PIN that would allow access to the account
- Social Security Number
- Taxpayer ID number
- Driver's license number or other ID number issued by any agency (student ID number)
- Passport number or other number issued by the US
- Individually identifiable health information except for education records covered by FERPA

Current Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- Statewide Product Standards
- Active Directory/Group Policy Objects
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Private Printing
- Locked Data Center
- Locked File Cabinets/Doors
- Limited Access (Need to Know)
- Removal of stale accounts
- Staff confidentiality and security training
- Video surveillance systems
- Strong password policy
- Single Sign-on for services
- External banners
- Environment snapshots
- Managed Internet Services

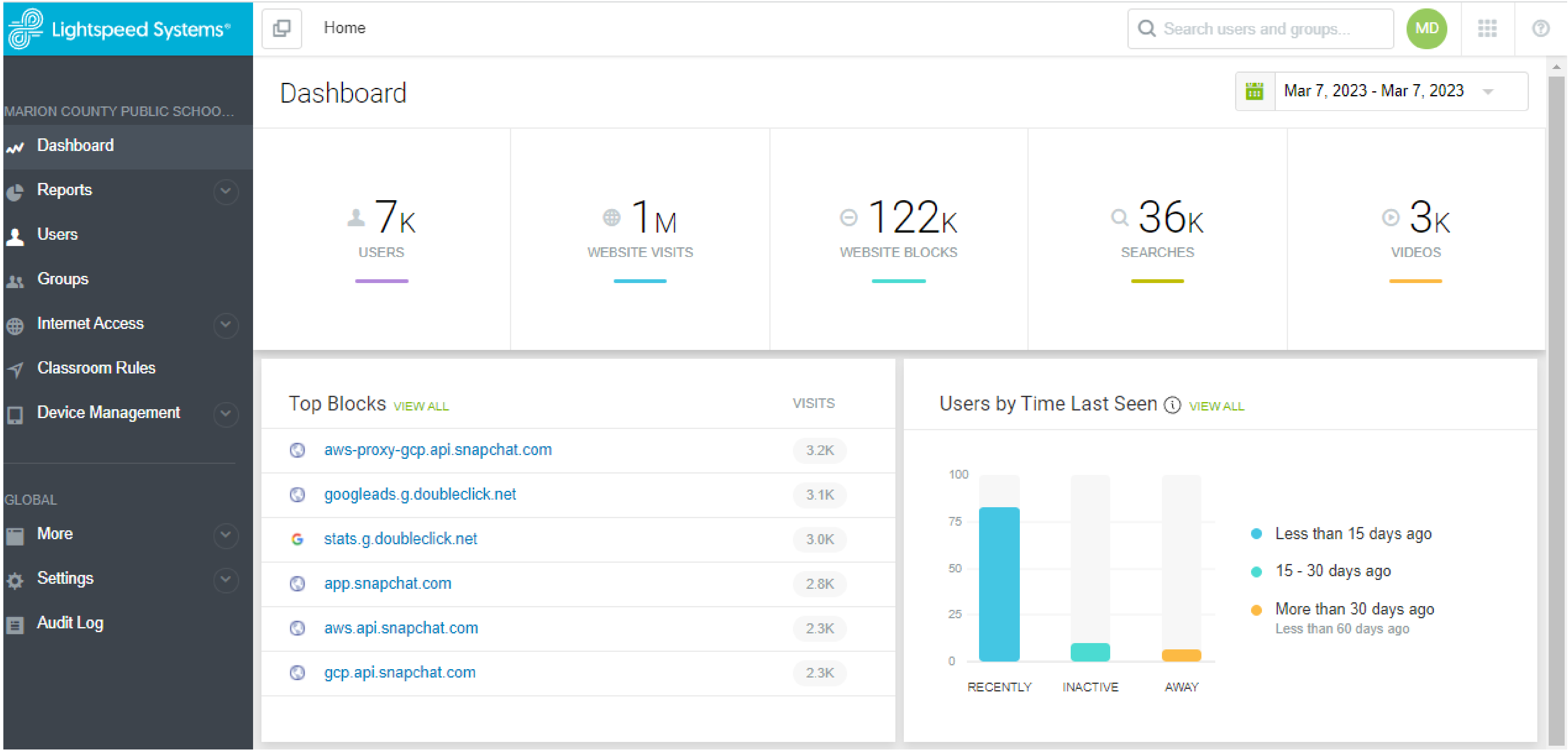
Implemented in 2022-23

- KETS Security Baseline Project:
  - Microsoft 365 Security Tools:
    - Self-Service Password Reset (SSPR)
    - Multi-Factor Authentication (MFA)
    - Conditional Access Policies
    - Password Expiration Notification
    - Advanced Security Reporting and Alerts

CIPA Requirements

- Children's Internet Protection Act (CIPA):
  - Requires use of internet filtering (Lightspeed)
    - Cloud based for mobile devices at home
    - Includes personal devices on WiFi
    - Key word searches
  - Education of minors in appropriate online behavior (social media, chat rooms, cyberbullying)
  - Acceptable Use Policy requirement for all accounts (08.2323 & 08.2323 AP 1)

Lightspeed Dashboard



Dashboard

Mar 7, 2023 - Mar 7, 2023

7K	1M	122K	36K	3K
USERS	WEBSITE VISITS	WEBSITE BLOCKS	SEARCHES	VIDEOS

Top Blocks VIEW ALL	VISITS
aws-proxy-gcp.api.snapchat.com	3.2K
googleads.g.doubleclick.net	3.1K
stats.g.doubleclick.net	3.0K
app.snapchat.com	2.8K
aws.api.snapchat.com	2.3K
gcp.api.snapchat.com	2.3K

Users by Time Last Seen ⓘ VIEW ALL

- ● Less than 15 days ago
- ● 15 - 30 days ago
- ● More than 30 days ago
  Less than 60 days ago

?