NOVEMBER 2024 ISSUE • Vol 16

IKON INSIGHTS

TECHNOLOGY NEWS FOR K-12 SCHOOLS

Brought to you by IKON EduTech Group, Inc.

IN THIS ISSUE

This monthly publication provided courtesy of IKON EduTech Group.

IKON is a premium IT consulting company focused on providing K-12 schools with customized technology solutions and personalized support.

Get More Free Tips, Tools and Services on Our Website:
www.ikonbusinessgroup.com
(212)334.6481

DON'T LET HOLIDAY TRAVEL COMPROMISE YOUR CYBERSECURITY

With the holiday season officially upon us, travel plans are in full swing – and so are cyber threats. Traveling for conferences, family vacations, or school events can inadvertently expose sensitive school data and systems to hackers. A single misstep, such as connecting to public WiFi or misplacing a device, can have far-reaching consequences for your school's cybersecurity. Here's how school leaders – from Executive Directors to IT Managers and Principals – can safeguard their schools' sensitive information during busy travel periods.

WHY K-12 SCHOOLS ARE A TARGET

Hackers often target schools because they hold valuable data, such as student records, financial information, and login credentials for critical systems. The risks are even higher during the holiday travel season when educators and staff may be less vigilant about cybersecurity.

According to World Travel Protection, only about 30% of organizations implement cybersecurity measures for employees on the go. For K-12 schools, this lack of preparation can lead to data breaches, disrupted operations, and loss of trust from parents and the community.

(continued on page 2)

DON'T LET HOLIDAY TRAVEL COMPROMISE YOUR CYBERSECURITY

(continued from page 1)

PRE-TRAVEL CYBERSECURITY CHECKLIST FOR K-12 STAFF

School leaders and IT administrators can significantly reduce risks by encouraging staff to follow these steps before traveling:

1. **Update All Devices** - Ensure laptops, tablets, and mobile devices are running the latest software to patch vulnerabilities.
2. **Back Up Important School Data** - Use secure cloud-based solutions to back up critical files, such as student records or lesson plans, in case a device is lost or stolen.
3. **Enable Multifactor Authentication (MFA)** - MFA adds a vital layer of security to school systems, making it harder for unauthorized users to gain access.
4. **Limit Access to Sensitive Systems** - Temporarily restrict access to student information systems or financial software for staff who don't need them while traveling.
5. **Encrypt and Secure Devices** - Ensure all school-issued devices are encrypted and password-protected to prevent unauthorized access to data.

TRAVELING SMART: BEST PRACTICES FOR K-12 STAFF ON THE GO

- **Avoid Public WiFi** - Public networks can expose school systems to hackers. If connecting is unavoidable, use a Virtual Private Network (VPN) to encrypt data traffic.
- **Be Wary of Public Charging Stations** - Attackers can exploit public USB ports to install malware or steal data. Staff should use their own chargers and connect directly to electrical outlets.
- **Secure Devices at All Times** - Keep devices with you or locked in a secure location. Consider using physical locks for laptops left in hotel rooms.
- **Disable Bluetooth When Not in Use** - Hackers can exploit Bluetooth connections to access devices. Staff should turn it off in public spaces.
- **Watch Out for Phishing and Scams** - Phishing emails and fraudulent online shopping sites are more common during the holidays. Train staff to recognize suspicious emails and avoid clicking on unverified links.

POST-TRAVEL CYBERSECURITY CHECK FOR K-12 STAFF

When school leaders and staff return from their travels, a few simple steps can help ensure their systems remain secure:

1. **Review Account Activity** - Check for unusual logins or unauthorized activity in school systems or personal accounts.
2. **Change Passwords** - Update passwords for any systems accessed during travel to mitigate potential security risks.
3. **Report Lost or Stolen Devices** - Establish a protocol for staff to immediately report missing school-issued devices to the IT team.

ESTABLISHING A SCHOOL-WIDE TRAVEL CYBERSECURITY POLICY

To protect school systems and data, K-12 administrators should implement a clear travel cybersecurity policy. This policy should:

- Define rules for accessing school networks and sensitive information while traveling
- Require the use of VPNs and other protective measures
- Outline steps for reporting and responding to lost or stolen devices
- Include training to help staff recognize phishing attempts and other common threats

STAY SECURE WITH IKON EDUTECH GROUP

At IKON EduTech Group, we're committed to helping K-12 schools safeguard student data and maintain compliance with regulations like Ed Law 2-D. Our team can help you implement solutions such as VPNs, encryption, and multifactor authentication to protect your school's data, even during peak travel seasons.

STUDENT DATA PRIVACY: WHY SCHOOLS SHOULD RETHINK EMAIL USERNAMES

PROPER EMAIL SYNTAX FOR STUDENTS: UNDERSTANDING NYSED LAW 2-D GUIDELINES

In the digital age, student email accounts are essential for education. However, New York State Education Law 2-D places stringent requirements on how personally identifiable information (PII), such as a student's name, is handled to ensure data privacy and security.

Today we'll explore the implications of including first and last names in school district email usernames and provides best practices for compliance.

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)?

Under Ed Law 2-D, PII is any information that can identify a student, including their name. While using a student's name for administrative purposes required by law is permissible, creating usernames for email accounts that directly include first and last names raises privacy concerns.

THE ROLE OF EMAIL SYNTAX IN STUDENT PRIVACY

A standard email address consists of three parts:

1. **Username:** Unique to the user (e.g., a student's name or nickname).
2. **"@" Symbol:** Separates the username from the domain.
3. **Domain Name:** Identifies the email service provider (e.g., schooldistrict.org).

School districts must carefully consider the username component, particularly if it includes PII like first and last names. While including a name might simplify identification within the school community, it could unintentionally expose sensitive data if shared externally.

BEST PRACTICES FOR STUDENT EMAIL SYNTAX

To comply with Ed Law 2-D and ensure data privacy:

- **Avoid Full Names in Usernames:** Instead of using a first and last name (john.smith@schooldistrict.org), consider using initials (js1234@schooldistrict.org) or unique numeric identifiers.
- **Follow Data Security Standards:** Adhere to industry best practices for privacy and security, such as encrypting emails and limiting access to student data.
- **Educate Stakeholders:** Ensure teachers, administrators, and students understand email use policies and the importance of protecting PII.

- **Consult Local Policies:** Each district may have additional guidelines from their Local Education Agency (LEA) or Internet Service Provider (ISP). Collaborate with your chief privacy officer or LEA counsel to align with these policies.

KEY TAKEAWAY

While using a student's full name in an email username is not explicitly prohibited, districts should avoid this practice to minimize data privacy risks. By implementing thoughtful email syntax and adhering to data security regulations under Ed Law § 2-D, schools can protect student information while fostering a safe digital learning environment.

Ensuring compliance with New York State Education Law 2-D is critical for protecting student data and fostering a secure learning environment. By implementing thoughtful email account practices, your school can meet privacy requirements while safeguarding sensitive information.

If your school's Data Protection Officer (DPO) needs additional support to navigate these complex regulations, IKON Edutech Group is here to help. Our DPO Compliance Support packages offer cost-effective solutions tailored to the unique challenges of K-12 schools. Let us assist your team in building a sustainable, long-term approach to compliance while you focus on delivering quality education.

We invite you to learn more about our DPO Compliance Support services and how we can help your school stay ahead in data protection.

Learn More

OUTDATED HARDWARE: WHAT TECHNOLOGY DIRECTORS NEED TO KNOW

As technology becomes central to K-12 education, schools must stay ahead of the risks posed by outdated hardware. Aging devices like Apple tablets, Android devices, and Chromebooks can leave a school's network exposed once they no longer receive OS updates, increasing the risk of vulnerabilities and potential data breaches. Here's what school technology directors need to know.

WHY OUTDATED HARDWARE POSES A RISK

While older devices may still function, they become a weak link in your network once their operating systems (OS) are no longer supported. Without regular updates, these devices lack protection against new security threats, including zero-day vulnerabilities that can leave them open to malicious access. According to recent statistics, 68 zero-day vulnerabilities were discovered in 2023—16 more than the previous year. This increase in threats underscores the importance of up-to-date hardware and timely patch deployment.

UNDERSTANDING UPDATE TIMELINES FOR COMMON DEVICES

Different types of devices come with varying timelines for OS updates. Here's a quick rundown:

- **Apple Devices:** Supported for about 7 to 9 years from their release date.
- **Samsung Android Tablets:** Supported for 4 years with automatic updates, as of August 2023.
- **Chromebooks:** For models released after 2021, Google provides automatic security updates for up to 10 years.

Knowing these timelines allows schools to anticipate when their devices will reach the end of their update cycle. Planning ahead helps ensure a smooth transition to new devices before significant security gaps appear.

ESTABLISHING A PATCH MANAGEMENT PROCESS

Implementing patches promptly is essential, especially for zero-day vulnerabilities. Best practice includes testing patches in a controlled environment before rolling them out district-wide to catch potential bugs and incompatibility issues. However, when a critical patch is released, timing is everything; too long a delay can leave systems vulnerable.

Consider the well-known Equifax breach in 2017, where a delay in patching a zero-day vulnerability led to the exposure of 143 million people's personal data. This example illustrates the critical nature of timely patch deployment, especially for older devices that may not automatically receive updates.

HOW IKON EDUTECH GROUP CAN HELP

Outdated hardware increases the risk of data breaches and compromises network security in schools. IKON EduTech Group specializes in providing customized technology solutions for K-12 schools, including Hardware Lifecycle Assessment, Patch Management Support, and Device Replacement Strategies. We work with schools to create sustainable device replacement plans aligned with your budget, helping to maintain a secure network environment.

ON-DEMAND WEBINAR:
SECURE YOUR CYBERSECURITY FUNDING - FCC PILOT PROGRAM PART 2

The FCC has launched a groundbreaking Cybersecurity Pilot Program to help schools and libraries bolster their cybersecurity defenses. This funding is critical, as cybercriminals continue to target educational institutions, putting sensitive data and essential networks at risk.

The program received over 2,700 applications—far exceeding the initial allocation. Now, the FCC has selected a diverse group of schools, libraries, and consortia to move forward in the competitive Part Two of the application process.

Watch Now

IKON is hosting a follow-up webinar to help you prepare for Part Two of the application and provide guidance on how to implement these critical cybersecurity funds effectively.