

August 2026

NNPS DIGITAL LEADERSHIP INITIATIVE

A CYBERSECURITY AWARENESS & PROFESSIONAL DEVELOPMENT SERIES

Back-to-School: Setting the Standard for Digital Leadership

As we prepare to welcome students back on August 24, we also reset our expectations for digital responsibility.

Cybersecurity is not just a technical safeguard. It is a professional standard.

The tone we set as administrators, teachers, and staff in our communication, device use, and digital habits directly influences student behavior. This year, we aim to move from basic cybersecurity awareness to active digital leadership.

This Month's Cyber Focus:

Modeling Secure Behavior:

Every school year brings new systems, new accounts, new tools, and renewed online activity. It also brings increased phishing attempts, impersonation emails, and fraudulent vendor communications.

Staff play a critical role in setting expectations by:

- Protecting district credentials with strong passwords and MFA
- Verifying unexpected requests through secondary channels
- Following approved AI tool guidance
- Safeguarding student data consistently
- Reporting suspicious activity promptly

Leadership in cybersecurity is not about technical expertise; it's about consistently modeling secure behaviors.

Students observe how adults manage devices, respond to emails, and protect information. Secure habits are contagious.

*Welcome Back,
Teachers and Staff!*

Common Warning Signs

Back-to-school season frequently includes:

- Phishing emails impersonating administrators or vendors
- Fake invoice or procurement requests
- Account verification messages requesting urgent action
- New tool suggestions that bypass formal approval processes
- AI tools requesting unnecessary permissions or access

If something appears urgent or unusual, pause and confirm through a known contact method.

One verified phone call can prevent a costly incident.

Security Spotlight

Convenience Should Never Replace Security

Writing student usernames and passwords on a label attached to a Chromebook may seem helpful, especially at the beginning of the school year.

However, if anyone can access the device, they also have access to the student's credentials.

Instead:

- Keep credentials in a secure location that is not attached to the device.
- Encourage students to learn their passwords whenever appropriate.
- Contact your site TSS if password assistance is needed.

A password only protects an account when it remains private.

August 2026

NNPS DIGITAL LEADERSHIP INITIATIVE

A CYBERSECURITY AWARENESS &
PROFESSIONAL DEVELOPMENT SERIES

Smart Habits That Help

Before we hit the ground running for this school year, let's take a few minutes to review some important reminders:

- **Never attach usernames or passwords directly to student devices.** Credentials should never be written on labels, sticky notes, or taped to Chromebooks, laptops, or monitors. ***Doing so defeats the purpose of password protection and could allow unauthorized access if a device is misplaced or accessed by others.***
- Review your password hygiene
- **Confirm MFA enrollment across district systems**
- Close unused browser tabs and active sessions
- **Remove unnecessary browser extensions**
- Ensure only approved applications are in use
- **Be mindful of classroom device visibility and screen sharing**

Strong systems support security, and individual habits reinforce it.

Security is strongest when it becomes a habit.

For Families

As students return to school, it is helpful to revisit:

- Expectations for responsible device use
- Appropriate online communication
- Responsible AI use for academic support
- Protecting personal information

Staff and families serve as partners in shaping a safe and responsible digital learning environment. Clear, consistent expectations across school and home environments create stability for students.

District Growth & Maturity

Over the past year, our division has strengthened:

- AI use & governance review processes
- Vendor privacy oversight
- Risk-based technology evaluations
- Cross-department cybersecurity collaboration

Cybersecurity is no longer an afterthought or a reactive measure. It is integrated into planning, instruction, and daily operations.

As we begin this academic year, we continue building a culture where secure behavior is the standard, not an option.



Final Thoughts

Digital leadership begins with setting the standard.

Every secure login, every verified email, every responsible data decision contributes to a stronger environment for our students and staff.

This year, we don't just practice cybersecurity; *we model it.*

Let's continue to raise the bar and lead by example, together.

Stay smart. Stay secure. Stay connected.

Until next time,

-Office of Information Security

Need help or have questions? Our Technology team is always here to support you.

<https://sbo.nn.k12.va.us/technology/>

tsc@nn.k12.va.us

(757) 881-5461 x.12411

