TECHNOLOGY COMMITTEE

DECEMBER 8, 2025

AGENDA

INFRASTRUCTURE

CYBER SECURITY

DEPARTMENT

NO UPDATES

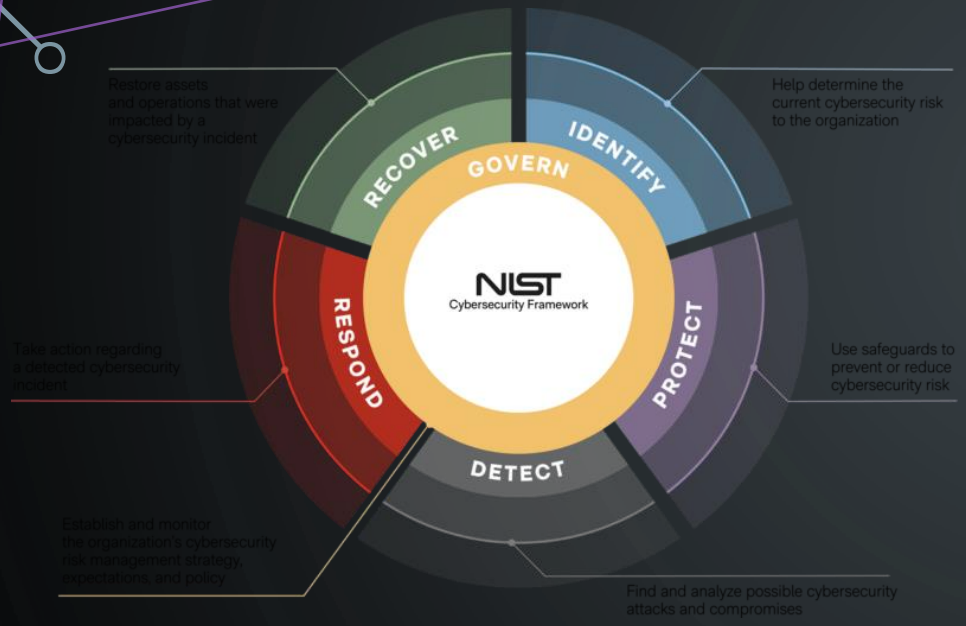
WEBSITE

AI CIRCLE UPDATE

INFRASTRUCTURE

- Previous meeting:
- Field technicians finishing up the Windows upgrades

- Updates:
  - PLTW Computer lab T106 will be upgraded to a laptop cart.
  - District will purchase AristotleK12 Licenses for all windows computers to pull analytics.



NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST Cybersecurity Framework 2.0

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood.

***GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management.*

The mission of the Wallkill Central School District, through an active partnership among school personnel, parents, students, and community, is to nurture individuals who value themselves and others; to develop learners who appreciate diversity as a resource; to provide an exemplary educational foundation that will foster the ability to think and communicate, and to encourage creativity, flexibility, and the continuous application of learning.

Cybersecurity is essential to protect student data, educational resources, and administrative systems.

Stakeholders include students, parents, staff, vendors, and regulatory bodies. We comply with FERPA, COPPA, and other applicable laws and regulations.

***GV.OC-02**: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.*

Internal Stakeholders & Expectations

1. **Executive Leadership (Superintendent, CIO, Board)**
   - Expectation: Cybersecurity strategy aligns with organizational mission and risk appetite.
   - Expectation: Regular reporting on risk posture and compliance status.
2. **IT Department**
   - Expectation: Implement technical controls (MFA, patching, network segmentation).
   - Expectation: Maintain incident response readiness and vulnerability management.
3. **Teachers & Staff**
   - Expectation: Clear acceptable use policies and training on phishing awareness.
   - Expectation: Easy access to secure systems without compromising usability.
4. **Students**
   - Expectation: Privacy of personal data and secure access to learning platforms.

External Stakeholders & Expectations

1. **Parents & Guardians**
   - Expectation: Protection of student data (FERPA compliance).
   - Expectation: Transparent communication on breaches or incidents.

1. **Vendors & Service Providers**
    - Expectation: Adherence to contractual cybersecurity requirements.
    - Expectation: Timely notification of security incidents affecting services.
2. **Regulatory Bodies**
    - Expectation: Compliance with laws (FERPA, COPPA, GDPR).
    - Expectation: Evidence of governance processes and risk management.
3. **Community Partners**
    - Expectation: Secure data sharing protocols for joint programs.

GV.OC-03: *Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed.*

Education Law 2D, PBOR, BOE Policy 5665

GV.OC-04*: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.*

Student Information System (SIS) Availability

- External Expectation: Parents and state agencies expect uninterrupted access to student records.
- Communication: Publish uptime commitments and incident response procedures.

Secure Data Exchange with Vendors

- External Expectation: Cloud service providers expect secure API integrations.
- Communication: Provide encryption standards and authentication requirements.

Compliance Reporting

- External Expectation: Regulatory bodies expect timely submission of compliance reports (FERPA, COPPA).
- Communication: Share reporting timelines and escalation contacts.

Learning Platform Access

- External Expectation: Students and parents expect 24/7 access to online learning tools.
- Communication: Document service level agreements (SLAs) and maintenance windows.

Incident Notification

- External Expectation: Vendors and partners expect immediate breach notifications.
- Communication: Define notification timelines and contact protocols in contracts.

***GV.OC-05**: Outcomes, capabilities, and services that the organization depends on are understood and communicated*

Cloud Hosting Services

- Dependency: Reliable uptime and secure infrastructure from a cloud provider.
- Communication: Document SLAs, backup procedures, and escalation contacts.

Internet Service Provider (ISP)

- Dependency: Continuous connectivity for learning platforms and administrative systems.
- Communication: Maintain ISP contact details and outage response plans.

Third-Party Learning Platforms

- Dependency: Secure and compliant access for students and staff.
- Communication: Share vendor compliance certifications and integration requirements.

Cybersecurity Threat Intelligence Feeds

- Dependency: Timely threat data for proactive defense.
- Communication: Define update frequency and integration into monitoring tools.

Payment Processing Services

- Dependency: Secure handling of financial transactions for tuition or fees.
- Communication: Ensure PCI compliance and breach notification protocols.

Sample policy: (GV.OC-05)

The organization shall maintain a comprehensive register of external dependencies that are critical to achieving its cybersecurity and operational objectives. This includes services, technologies, and capabilities provided by third-party vendors, partners, and service providers.

Requirements:

1. **Identification:**
    - All external services essential for organizational operations (e.g., cloud hosting, internet connectivity, learning platforms , payment processing) must be identified and classified based on criticality.
2. **Documentation:**
    - Maintain a **Dependency Register** that includes:
        - Service name and provider
        - Description of dependency

- Associated risks and mitigation measures
- Service Level Agreements (SLAs) and compliance obligations
- Contact and escalation details

1. **Communication:**
    - Share dependency information with internal stakeholders responsible for risk management, incident response, and governance.
    - Ensure that contingency plans for critical dependencies are communicated and tested regularly.
2. **Review and Update:**
    - Review the Dependency Register at least annually or upon significant changes in services or vendors.
    - Update governance documentation to reflect changes in external dependencies.

Accountability:
The Chief Information Security Officer (CISO) or designated governance lead is responsible for maintaining and communicatingthe Dependency Register.

WEBSITE

TRANSLATION WITH WEGLOT

FROM/TO	TOTAL TRANSLATED WORDS	MANUALLY TRANSLATED WORDS			
English > Spanish	19,187	0%	Options		
English > French	8,710	0%	Options		
English > Traditional Chinese	8,292	0%	Options		
English > Russian	6,757	0%	Options		
English > Portuguese	5,993	0%	Options		
English > Swahili	1,769	0%			

WEGLOT

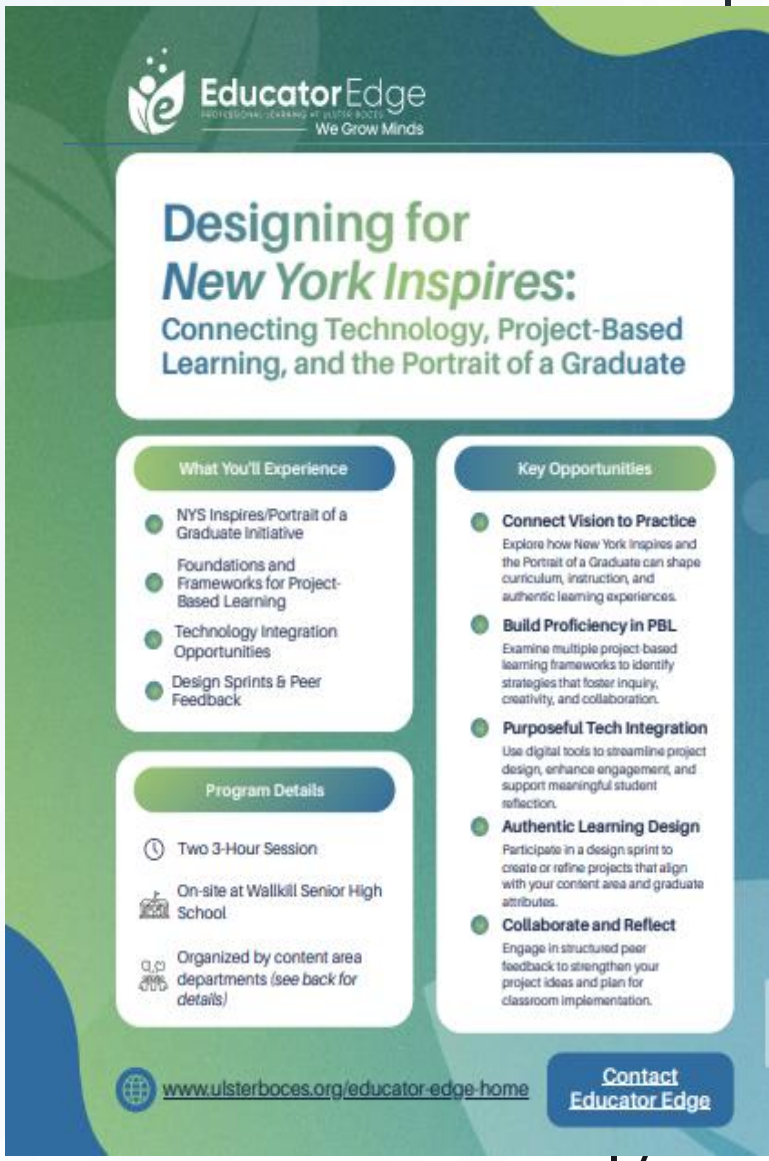
Athletics Manager

ARISTOTLE K-12 PROFESSIONAL DEVELOPMENT

- Initial PD sessions will be organized for faculty, focusing on classroom management with AristotleK12BC.
- Each session will last for 1 hour.
- Separate sessions will be scheduled for Primary and Secondary levels to accommodate different groups.
- A self-paced option is under consideration, featuring an 18-minute instructional video.
- Participants completing the self-paced session will receive ½ hour of CTLE credit, reflecting the shorter duration.

TECHNOLOGY INTEGRATION SPECIALIST UPDATE:

- **Connect Vision to Practice**
- Explore NYS Inspires and Portrait of a Graduate initiatives
- Foundations for Project-Based Learning (PBL)
- Integrate Meaningful Technology into Lesson Design
- **Session 1: Introduction & Exploration (2/10/26-2/13/26)**
- Build community and establish session norms
- Examine and select PBL frameworks for departmental use
- Begin designing small-scale projects with digital tools
- **Session 2: Ideation, Tuning, and Reflection 3/10/26-3/13/26)**
- Develop ready-to-implement PBL units or mini-projects
- Participate in design sprints and structured peer feedback
- Refine project plans and plan for classroom rollout
- **Purposeful Technology Integration**
- Use digital tools to streamline project design/boost student reflection
- Apply technology in discipline-specific ways
- **Collaboration & Reflection**
- Engage in peer feedback and collaborative planning
- Reflect on growth and plan for continued learning
- Interdisciplinary Project Design



PD FOR ALL HIGH SCHOOL INSTRUCTIONAL STAFF 9-12

UPDATING OUR TECHNOLOGY PLAN (2026-2029)

- Plan must be submitted to NYSED by July 1, 2026 (effective Sept 2026–June 2029)
- Submission is through the NYSED online portal (SED Monitoring system)
- Plan must address:
  - Vision & goals for technology integration
  - Equitable access to devices and connectivity
  - Professional development for staff
  - Secure, reliable infrastructure
  - Alignment with NYSED standards
  - Plan is required for state technology funding (e.g., Smart Schools Bond Act)
- Approved plan will be posted on the district website

AI CIRCLE UPDATE

WALLKILL CSD IS ACTIVELY PARTICIPATING IN THE AI CIRCLE, A COLLABORATIVE INITIATIVE DESIGNED TO HELP DISTRICTS DEVELOP AND REFINE A DISTRICT-WIDE VISION FOR RESPONSIBLE AI USE—ENHANCING BOTH STUDENT LEARNING AND INSTRUCTOR EFFICACY.

Date & Time: Tuesday, December 9, 4:00–6:00 p.m. (Virtual Tuning Session)

Format:

- Districts are paired to participate in two complete 40-minute Dilemma Tuning Protocols.
- Each district presents its essential question and current work.
- Each district serves as a "critical friend," providing thoughtful, kind, and specific feedback to their partner district.
- Both teams receive dedicated time for presentation and valuable peer perspectives.

What We're Preparing:

- Our essential question(s) for AI implementation in Wallkill CSD.
- A clearly framed question for our critical friends.
- Brief context or materials to share with our partner district.

Session Agenda:

1. Brief review of the Dilemma Tuning Protocol.
2. Wallkill CSD presents its essential question and work.
3. Partner district presents; Wallkill serves as critical friend.
4. Collaborative feedback and insights.
5. Reflection and next steps.

Why This Matters:

- Fosters cross-district collaboration and shared learning.
- Ensures our AI vision is robust, actionable, and aligned with best practices.
- Builds capacity for responsible, effective AI integration in our schools.