Draft

Delphos City Schools
CYBERSECURITY POLICY

Adopted: [Date]
Last Reviewed: [Date]
Responsible Role: Technology Coordinator

---

1. PURPOSE

The purpose of this Cybersecurity Policy is to establish a comprehensive cybersecurity program in compliance with Ohio House Bill 96 (Ohio Revised Code §9.64) and to protect the confidentiality, integrity, and availability of District information systems and data.

This policy establishes governance, security controls, incident response procedures, training requirements, and reporting obligations applicable to all District technology resources.

---

2. SCOPE

This policy applies to:

- All District employees, contractors, volunteers, and third parties with access to District systems
- All District-owned or managed devices
- All cloud services and third-party systems used to store or process District data
- All student, employee, financial, and operational data

District Technology Environment

The District serves approximately 900 students and 200 staff across three buildings:

- Elementary School
- Middle School
- High School

The District operates primarily in a cloud-based environment, utilizing third-party hosted systems for instructional, administrative, and operational functions.

The District maintains a Windows Server environment (Active Directory, DNS, DHCP) that is hosted offsite and managed by the District's Information Technology Center (ITC). The ITC is responsible for server hosting and backups under separate agreement.

This policy governs both District-managed systems and cloud-based services used to conduct District business.

---

3. CYBERSECURITY FRAMEWORK ALIGNMENT

The District cybersecurity program is aligned with the following recognized standards:

- NIST Cybersecurity Framework (CSF)

- CIS Critical Security Controls (as applicable to K–12 environments)

The District will use these frameworks to guide risk management, security control implementation, and continuous improvement.

---

4. GOVERNANCE AND RESPONSIBILITIES

4.1 Board of Education

- Formally adopts this Cybersecurity Policy and any subsequent revisions.
- Provides governance oversight of cybersecurity risk.
- Approves ransomware payment decisions when applicable.
- Receives incident summaries and compliance updates as required by law.

4.2 Superintendent

- Provides executive oversight of cybersecurity risk.
- Ensures administrative enforcement of this policy.
- Ensures compliance with state reporting requirements.

4.3 Technology Coordinator

- Implements and maintains the cybersecurity program.
- Conducts and documents annual risk assessments.
- Maintains current system and data inventories.
- Manages security controls and monitoring.
- Leads incident response and reporting.
- Maintains compliance documentation and evidence for audit purposes.
- Coordinates cybersecurity responsibilities with the ITC and third-party vendors.

4.4 Shared Responsibility Model

The District operates under a shared responsibility model for cybersecurity.

District Responsibilities: - Endpoint security and device management within all three buildings. - User account management and access control decisions. - Security configuration of District-managed network equipment and wireless infrastructure. - Vendor review and approval for cloud-based applications. - Staff cybersecurity training and awareness. - Incident identification, coordination, documentation, and required state reporting.

ITC Responsibilities (Per Service Agreement): - Hosting and infrastructure management of the Windows Server environment (Active Directory, DNS, DHCP). - Backup operations for hosted server infrastructure. - Infrastructure-level security controls within the hosted environment.

The District shall maintain written agreements or memoranda of understanding defining ITC security and backup responsibilities. Responsibility boundaries shall be reviewed annually to ensure clarity and audit defensibility.

---

5. RISK MANAGEMENT

The District shall:

- Maintain an inventory of hardware, software, cloud services, and data systems across all three buildings.
- Conduct periodic risk assessments to identify vulnerabilities in both cloud-based and on-premise/network infrastructure.
- Coordinate with the ITC regarding risks related to the hosted Windows Server environment.
- Implement safeguards appropriate to District size (900 students, 200 staff), distributed building model, and risk exposure.
- Prioritize protection of sensitive data including student records (FERPA), personnel records, financial data, and authentication systems.

Risk assessments shall be documented and reviewed annually.

---

6. SECURITY CONTROLS

The District shall implement reasonable administrative, technical, and physical safeguards, including but not limited to:

6.1 Access Control

- Unique user accounts for all staff.
- Role-based access control.
- Multi-factor authentication (MFA) where feasible.
- Timely removal of access upon separation.

6.2 Endpoint and Network Security

- Managed antivirus/endpoint protection on all District-issued devices.
- Regular operating system and application patching.
- Firewall and content filtering systems protecting all three buildings.
- Secure Wi-Fi configuration at each building.
- Coordination with the ITC for security controls related to the hosted Windows Server (Active Directory, DNS, DHCP).

6.3 Data Protection

- Regular data backups (including offline or immutable backups).
- Encryption of sensitive data where feasible.
- Secure cloud configuration practices.

6.4 Vendor and Third-Party Risk

- Review of vendor security practices prior to adoption, particularly for cloud-based educational platforms.
- Verification of data privacy agreements and Student Data Privacy Addendums where required.
- Periodic review of ITC service agreements to ensure backup and security responsibilities are clearly defined.

---

7. INCIDENT RESPONSE AND REPORTING

7.1 Incident Definition

A cybersecurity incident includes unauthorized access, ransomware, malware infection, data breach, system compromise, or disruption of District operations.

7.2 Response Procedures

The District shall maintain a documented Incident Response Plan that includes:

1. Identification and containment
2. Investigation and documentation
3. Eradication and recovery
4. Post-incident review

7.3 State Reporting Requirements

In accordance with Ohio House Bill 96:

- Report qualifying cybersecurity incidents to the appropriate state authority within seven (7) days.
- Maintain documentation of incident details and corrective actions.

7.4 Ransomware Payments

Any ransomware payment must:

- Receive prior approval from the Board of Education.
- Be documented as serving a public interest purpose.
- Be reported as required by state law.

---

8. SECURITY AWARENESS TRAINING

The District shall provide annual cybersecurity awareness training to all employees with access to District systems.

Training shall include:

- Phishing awareness
- Password security
- Data privacy responsibilities
- Incident reporting procedures

Training completion shall be documented and retained for compliance purposes.

---

9. BUSINESS CONTINUITY AND BACKUPS

The District shall:

- Maintain regular backups of critical systems and data.
- Test restoration procedures periodically.

- Develop procedures to maintain operational continuity during system disruptions.

10. DOCUMENTATION AND RECORDKEEPING

The Technology Coordinator shall maintain written and electronic documentation sufficient to demonstrate compliance with Ohio Revised Code §9.64 and this policy.

Documentation shall include, at minimum:

- Annual risk assessments and remediation plans
- Current hardware, software, and cloud service inventories
- Security control implementation records
- Incident logs and investigative summaries
- State reporting confirmations
- Training completion records
- Board approvals and policy revisions
- ITC agreements and service documentation

Documentation shall be retained in accordance with District records retention policies and shall be organized in a manner that allows timely production during audits, public records requests, insurance reviews, or post-incident investigations.

11. POLICY REVIEW AND UPDATES

This policy shall be reviewed annually and updated as necessary to address evolving threats, technology changes, and legal requirements.

12. ENFORCEMENT

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment and legal action where appropriate.

CERTIFICATION

The Board of Education of Delphos City Schools hereby adopts this Cybersecurity Policy in compliance with Ohio House Bill 96 and Ohio Revised Code §9.64.

Board President: _____ Date: _____

Treasurer: _____ Date: _____

Superintendent: _____ Date: _____

Draft

Delphos City Schools
12-Month Cybersecurity Roadmap

Prepared By: Technology Coordinator
Roadmap Period: _____

PURPOSE

This 12-Month Cybersecurity Roadmap provides a structured improvement plan aligned to:

- Ohio HB 96 compliance requirements
- Delphos City Schools Cybersecurity Policy
- NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)
- District size and one-person technology department model

This roadmap prioritizes high-impact, manageable improvements across one year.

QUARTER 1 – FOUNDATION & GOVERNANCE

1. Policy & Documentation Finalization

☐ Board adoption of Cybersecurity Policy
☐ Board adoption of Incident Response Plan
☐ Complete Annual Risk Assessment
☐ Establish centralized compliance documentation folder structure

2. Access Control Hardening (NIST PR.AC)

☐ Review all administrative accounts (AD + cloud)
☐ Reduce unnecessary elevated privileges
☐ Enforce MFA for all staff where available
☐ Implement documented quarterly account review process

3. Backup Verification (NIST RC.RP)

☐ Meet with ITC to review server backup procedures
☐ Document shared responsibility boundaries
☐ Verify backup retention periods
☐ Perform or document restore test verification

QUARTER 2 – PROTECTION IMPROVEMENTS

4. Endpoint Security Review (NIST PR.IP)

- ☐ Verify endpoint protection on all district devices
- ☐ Evaluate EDR solution feasibility (budget dependent)
- ☐ Confirm automatic OS and software patching

5. Cloud Security Review (NIST PR.IP)

- ☐ Review security settings for primary cloud platforms
- ☐ Confirm MFA enforcement
- ☐ Review data sharing settings and external access policies

6. Vendor & Third-Party Risk Review

- ☐ Review top 10 critical vendors
- ☐ Confirm data privacy agreements on file
- ☐ Document vendor security review checklist

QUARTER 3 – DETECTION & RESPONSE MATURITY

7. Logging & Monitoring (NIST DE.CM)

- ☐ Confirm firewall log retention
- ☐ Document log review procedure
- ☐ Identify alert escalation workflow

8. Incident Response Exercise (NIST RS)

- ☐ Conduct one tabletop exercise (ransomware scenario)
- ☐ Document findings and corrective actions
- ☐ Update IR Plan if needed

9. Phishing & Awareness Reinforcement

- ☐ Conduct annual cybersecurity training
- ☐ Run at least one phishing simulation (if platform available)
- ☐ Document staff completion rates

QUARTER 4 – RECOVERY & STRATEGIC REVIEW

10. Disaster Recovery Review (NIST RC)

- ☐ Review recovery priorities for SIS, finance, and instructional systems
- ☐ Document Recovery Time Objectives (RTO)
- ☐ Validate contact lists and escalation tree

11. Insurance & Legal Review

☐ Review cyber liability policy coverage limits
☐ Document carrier incident notification requirements
☐ Align reporting timelines with HB 96

12. Annual Program Review

☐ Re-evaluate risk assessment
☐ Document improvements achieved
☐ Identify next year's priorities
☐ Provide summary update to Superintendent / Board

MATURITY GOALS BY YEAR END

By the end of the 12-month period, Delphos City Schools should be able to demonstrate:

✔Documented cybersecurity governance
✔Annual risk assessment completion
✔MFA enforcement for staff
✔Verified backup and recovery capability
✔Conducted tabletop exercise
✔Documented vendor review process
✔Evidence of cybersecurity training
✔Defined incident reporting workflow compliant with HB 96

RESOURCE CONSIDERATIONS (ONE-PERSON DEPARTMENT MODEL)

This roadmap is designed to:

- Avoid major infrastructure overhauls
- Prioritize documentation and defensibility
- Focus on high-risk, high-impact improvements
- Spread workload evenly across quarters

Adjust timelines as operational demands require.

Technology Coordinator: _____ Date: _____

Draft

Delphos City Schools
Cybersecurity Incident Response Plan (IRP)

Effective Date: [Date]
Last Reviewed: [Date]
Responsible Role: Technology Coordinator

---

1. PURPOSE

This Incident Response Plan (IRP) establishes the procedures Delphos City Schools will follow to identify, respond to, contain, investigate, report, and recover from cybersecurity incidents in compliance with Ohio House Bill 96 (Ohio Revised Code §9.64).

This plan supports the District Cybersecurity Policy and is designed to protect the confidentiality, integrity, and availability of District systems and data.

---

2. SCOPE

This plan applies to all cybersecurity incidents affecting:

- District-owned devices
- District networks across all three buildings (Elementary, Middle, High School)
- Cloud-based systems used by the District
- The ITC-hosted Windows Server environment (Active Directory, DNS, DHCP)
- Student, employee, financial, and operational data

---

3. INCIDENT DEFINITION

A cybersecurity incident includes, but is not limited to:

- Unauthorized access to systems or data
- Ransomware infection
- Malware outbreak
- Phishing compromise
- Data breach or suspected data exfiltration
- Denial of service attack
- Significant disruption to instructional or operational systems

Any staff member who suspects a cybersecurity incident must immediately report it to the Technology Coordinator.

---

4. ROLES AND RESPONSIBILITIES

4.1 Technology Coordinator

- Serves as Incident Response Lead

- Confirms and classifies incidents
- Coordinates containment and recovery actions
- Communicates with ITC as necessary
- Documents all incident details
- Ensures required state reporting within seven (7) days

4.2 Superintendent

- Provides executive oversight
- Assists with communication decisions
- Notifies Board leadership when appropriate

4.3 ITC

- Assists with incidents involving hosted Windows Server infrastructure
- Provides forensic or infrastructure-level support as defined in service agreements

4.4 Board of Education

- Approves ransomware payments when required
- Receives post-incident summary reports

---

5. INCIDENT RESPONSE PROCESS

Phase 1: Identification

- Receive report or detect abnormal system behavior
- Determine scope and severity
- Preserve logs and relevant evidence
- Begin incident documentation log

Phase 2: Containment

- Isolate affected devices or accounts
- Disable compromised credentials
- Block malicious IP addresses or domains if applicable
- Coordinate with ITC if server infrastructure is affected

Phase 3: Eradication

- Remove malware or unauthorized access mechanisms
- Patch vulnerabilities
- Reset passwords and enforce MFA where applicable

Phase 4: Recovery

- Restore systems from verified backups
- Validate system integrity
- Monitor for signs of reinfection or continued compromise

Phase 5: Post-Incident Review

- Document root cause analysis
- Identify control improvements

- Update policies or safeguards as needed
- Provide summary report to Superintendent and Board

---

6. INCIDENT DOCUMENTATION REQUIREMENTS

The Technology Coordinator shall maintain a written incident record including:

- Date and time of detection
- Nature of the incident
- Systems affected
- Data potentially impacted
- Actions taken
- Recovery steps
- Notification and reporting actions
- Lessons learned

Documentation shall be retained according to District records retention policies.

---

7. STATE REPORTING REQUIREMENTS (HB 96)

In accordance with Ohio Revised Code §9.64:

- Qualifying cybersecurity incidents shall be reported to the appropriate state authority within seven (7) days of confirmation.
- Reports shall include sufficient detail to describe the nature and scope of the incident.
- Documentation of the report and confirmation of submission shall be retained.

The Technology Coordinator is responsible for ensuring timely reporting.

---

8. RANSOMWARE RESPONSE PROCEDURES

If ransomware is detected:

1. Immediately isolate affected systems.
2. Preserve evidence.
3. Notify Superintendent.
4. Contact ITC for infrastructure coordination.
5. Assess backup viability.

No ransomware payment shall be made without:

- Formal Board of Education approval
- Documentation that payment serves a public interest purpose
- Compliance with all state reporting requirements

---

9. COMMUNICATION PROTOCOL

Internal communication shall follow this order:

1. Technology Coordinator
2. Superintendent
3. Board Leadership (as appropriate)
4. Legal Counsel (if required)

External communication (parents, staff, media) shall be coordinated through the Superintendent.

---

10. TESTING AND REVIEW

This Incident Response Plan shall be:

- Reviewed annually
- Updated following significant incidents
- Tested periodically through tabletop exercises when feasible

---

11. INCIDENT SEVERITY CLASSIFICATION MATRIX

Incidents shall be classified to ensure appropriate response and reporting urgency.

Low: - Isolated malware infection - Single compromised user account - No evidence of data exposure

Moderate: - Multiple affected devices - Limited operational disruption - Potential exposure of non-sensitive data

High: - Confirmed unauthorized access to sensitive data (FERPA, personnel, financial) - Widespread phishing compromise - Significant disruption to instructional operations

Critical: - Ransomware affecting multiple systems - Confirmed data exfiltration of protected information - District-wide operational shutdown - Incident requiring law enforcement involvement

High and Critical incidents require immediate Superintendent notification and evaluation for state reporting under HB 96.

---

12. SEVEN-DAY STATE REPORTING CHECKLIST (HB 96)

Upon confirmation of a qualifying incident:

☐ Confirm incident classification (High or Critical).
☐ Document date/time of confirmation (start of 7-day clock).
☐ Notify Superintendent.
☐ Coordinate with ITC if infrastructure involved.
☐ Gather incident details (systems affected, data involved, scope).
☐ Prepare state reporting documentation.
☐ Submit report to appropriate state authority within seven (7) days.
☐ Retain confirmation of submission.
☐ Provide summary to Board leadership.

This checklist shall be retained with incident documentation.

---

13. QUICK RESPONSE REFERENCE (DESK COPY)

If you suspect ransomware or major breach:

1. Disconnect affected device(s) from network immediately.
2. Do NOT power off unless encryption is actively spreading.
3. Preserve logs and screenshots if possible.
4. Reset compromised credentials.
5. Notify Superintendent.
6. Contact ITC (if server-related).
7. Begin incident log.
8. Evaluate need for state reporting.

Keep this reference accessible at all times.

---

14. TABLETOP EXERCISE TEMPLATE

To demonstrate compliance and readiness, the District shall conduct periodic tabletop exercises when feasible.

Exercise Documentation Template:

- Date of Exercise:
- Scenario Used (e.g., ransomware, phishing compromise):
- Participants:
- Timeline of Simulated Events:
- Decisions Made:
- Communication Actions:
- Gaps Identified:
- Corrective Actions Assigned:
- Follow-Up Completion Date:

Completed tabletop documentation shall be retained as evidence of annual review and testing.

---

15. PLAN APPROVAL

This Incident Response Plan is adopted by Delphos City Schools in support of compliance with Ohio House Bill 96 and District Cybersecurity Policy.

Superintendent: _____ Date: _____

Technology Coordinator: _____ Date: _____

Technology Coordinator: _____ Date: _____

Draft

Delphos City Schools
Annual Cybersecurity Risk Assessment Template

Assessment Year: _____
Assessment Conducted By: Technology Coordinator
Date Completed: _____
Next Review Date: _____

---

1. PURPOSE

This Cybersecurity Risk Assessment is conducted annually in accordance with Ohio Revised Code §9.64 (HB 96) and the Delphos City Schools Cybersecurity Policy.

The purpose of this assessment is to:

- Identify cybersecurity risks to District systems and data
- Evaluate the likelihood and impact of identified risks
- Document existing safeguards
- Identify remediation actions and priorities
- Provide documentation for audit and compliance purposes

---

2. DISTRICT TECHNOLOGY PROFILE

Student Enrollment: ~900

Staff: ~200

Buildings: Elementary, Middle School, High School

Technology Environment Summary

- Cloud-based instructional and administrative systems
- ITC-hosted Windows Server (Active Directory, DNS, DHCP)
- District-managed network infrastructure across three buildings
- District-issued staff and student devices

---

3. ASSET INVENTORY SUMMARY

Attach or reference current inventories for:

☐ Hardware (servers, switches, firewalls, endpoints)
☐ Software applications
☐ Cloud platforms
☐ Critical data systems (SIS, EMIS, payroll, finance)
☐ Backup systems

Inventory Location: _____

---

4. RISK IDENTIFICATION AND ANALYSIS

Use the table below to document identified risks.

#	Risk Description	Affected System	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Existing Controls	Residual Risk	Remediation Needed	Target Date
1	Phishing leading to credential compromise (NIST PR.AC / PR.AT)	Staff Email / Cloud Accounts	Med	High	MFA enabled, annual training	Med	Increase phishing simulations	Q4
2	Ransomware infection via endpoint device (NIST PR.IP / DE.CM)	Student / Staff Devices	Med	High	Endpoint protection, content filter	Med	Evaluate EDR solution	Q3
3	Unauthorized access to student records (FERPA exposure) (NIST PR.AC)	SIS / Cloud Data Systems	Low	High	Role-based access control	Low	Quarterly access review	Ongoing
4	Cloud service misconfiguration (NIST PR.IP)	Cloud Platforms	Med	Med	Vendor configuration review	Med	Annual security review checklist	Q2
5	Backup failure or inability to restore (NIST RC.RP)	ITC Hosted Server / Cloud Data	Low	High	ITC-managed backups	Low	Annual restore test verification	Q2
6	Lack of logging or monitoring visibility (NIST DE.CM)	Network / Server Logs	Med	Med	Firewall logs retained	Med	Implement centralized log review process	Q4
7	Insider misuse of privileges (NIST PR.AC)	Active Directory / Cloud Admin	Low	High	Limited admin accounts	Low	Annual privilege review	Q1

Additional risks should be documented below:

#	Risk Description	Affected System	Likelihood	Impact	Existing Controls	Residual Risk	Remediation Needed	Target Date

Common Risk Categories to Evaluate (Aligned to NIST CSF Functions):

Identify (ID): Asset inventory gaps, undocumented systems, vendor risk

Protect (PR): Weak passwords, lack of MFA, inadequate endpoint protection, poor network segmentation

Detect (DE): Insufficient logging, lack of alert monitoring, delayed incident detection

Respond (RS): Undefined escalation procedures, communication delays

Recover (RC): Untested backups, incomplete disaster recovery documentation

- Physical security of network equipment

---

5. HIGH-RISK FINDINGS SUMMARY

List any risks rated High Likelihood + High Impact or requiring priority action.

---

6. REMEDIATION PLAN

For identified high or moderate risks, document corrective actions.

Risk #	Corrective Action	Responsible Party	Budget Impact	Completion Target	Status

---

7. ITC COORDINATION REVIEW

☐ Reviewed ITC-hosted infrastructure responsibilities
☐ Verified backup procedures for Windows Server
☐ Confirmed shared responsibility boundaries
☐ Reviewed service agreement documentation

Notes: _____

---

8. TRAINING AND AWARENESS REVIEW

☐ Annual cybersecurity training completed
☐ Phishing awareness included
☐ Incident reporting process reviewed with staff
☐ Training records retained

---

9. INSURANCE AND LEGAL REVIEW

☐ Cyber liability insurance coverage reviewed
☐ Coverage limits adequate
☐ Incident notification requirements documented

---

10. EXECUTIVE SUMMARY

Summarize overall cybersecurity posture for the assessment year:

- Overall Risk Level: Low / Moderate / Elevated / High
- Major Improvements Since Last Year:
- Areas Needing Continued Attention:

Summary Narrative:

11. CERTIFICATION

I certify that this annual cybersecurity risk assessment was conducted in good faith and reflects the current cybersecurity posture of Delphos City Schools.

Technology Coordinator: _____ Date: _____

Superintendent Review: _____ Date: _____

AI in Education: Model Policy for Ohio Districts and Schools

I. PURPOSE STATEMENT

To support students and educators in the use of artificial intelligence (AI) for educational and operational purposes, the Board of Education of **Delphos City Schools** has created this policy on the use of AI. The purpose of this policy is to prepare students for success, encourage innovation for classroom instruction, and embrace opportunities for operational efficiency, while providing for consistent expectations, standards, and approval processes for safe and responsible implementation and integration of AI. This applies to multiple use cases, applications, and integration of AI, including generative AI.

II. DEFINITIONS

- **Artificial intelligence (AI):** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.[1]
- **Generative AI:** Any internet-based generative artificial intelligence programs that make use of large language model algorithms to make something new. AI used for auto-complete, minor text predictions, and/or grammar/spelling/punctuation suggestions, commonly found in most word-processing applications, is not considered generative AI.[2]
- **AI tool:** AI applications, algorithms, or systems that make use of AI to generate outputs based on human inputs, with an emphasis on generative AI.[3]

III. AI LITERACY

The Board recognizes the importance of preparing students and educators for the successful integration of innovative technologies. Accordingly, it is the policy of the Board that

---

[1] 15 U.S. Code § 9401, Sec. 3

[2] O.A.C. 3342-3-01.8(B)(15)

[3] Ohio School Boards Association (OSBA), Sample Policy EDEC: Artificial Intelligence

Delphos City Schools responsibly integrate AI by building AI literacy for all students and educators, including integration of AI into relevant curriculum, professional learning opportunities, and safe and responsible usage.

IV. STAKEHOLDER ENGAGEMENT

[An ongoing AI workgroup shall be convened/The scope of a related, existing workgroup should be revised] to inform AI policy and implementation. The workgroup should include educators who are representative of grade levels and departments, including special education and related services professionals, other relevant staff, Board members, and students, as well as external representatives such as local businesses and postsecondary institutions. Educators and staff should be given the opportunity to explore and gain experience with applications and integrated approaches to achieving **Delphos City Schools** priorities. The workgroup should regularly review new research and guidance and provide ongoing feedback to the **Delphos City Schools**.

Parents and community members should be informed through ongoing engagement about the skills students need for the future workforce and how AI is being used in the classroom. Educational resources may be provided to empower families to understand the potential risks associated with the unsupervised use of AI tools. Regular AI updates, including use of tools and opportunities for feedback, shall be integrated into the existing family and community engagement strategy.

V. DATA PRIVACY AND SECURITY

The **Delphos City Schools** is committed to protecting the privacy and security of all student and staff data. The adoption and implementation of any AI tool must adhere to existing data privacy and security policies that include, but are not limited to, Personally Identifiable Information (PII), FERPA, and any other relevant state of Ohio and federal laws. AI tools should only access, store, or process data that is necessary, and must do so in a secure, transparent, and ethical manner. AI systems must be vetted to ensure they meet rigorous standards for data encryption, access control, and responsible data use.

Users must also follow the terms of service, including appropriate age limits.

DRAFT

VI. PROCUREMENT AND EVALUATION OF AI TOOLS

The adoption of AI-enabled tools should be conducted in accordance with existing procurement policies and in alignment to the **Delphos City Schools** core values, goals, and priorities. Selection procedures must ensure that any AI tool must adhere to data privacy and security policies. Evaluation of tools must also address alignment to instructional and operational goals, accessibility, and cost. All third-party vendors providing AI tools must comply with **Delphos City Schools** standards, state and federal law for data protection, ethical use, and accessibility.

VII. ETHICAL USE OF AI

It is the policy of the **Delphos City Schools** that the design and implementation of AI be safe, responsible, and keep people at the core of every AI-related decision. AI implementation should be human-centered and should empower students, educators, and communities. It is a tool to support learning and teaching, not a substitute for student effort or the role of the educator. Accordingly, users should critically analyze AI output, respect safeguards and rules, and be transparent about its use.

VIII. ACCEPTABLE USE

The **Delphos City Schools** recognizes that responsible and appropriate uses of AI by students and educators will vary depending on the context, including but not limited to grade level, subject, and/or the nature of the classroom activity or assignment.

Expectations for acceptable student uses should be clearly articulated by educators in alignment with policy and guided by the specific requirements for an assignment or activity. This includes specifying AI use expectations in course syllabi and assignment instructions when relevant. These expectations should clearly articulate the expectations of use, types of relevant assignments where AI use is acceptable, and required format for references.

Educators should consider the impact on learning objectives and assessment of student learning when designing related instruction and classroom activities. No assignment shall require the use of a tool that cannot be provided by the **Delphos City Schools.** AI tools approved for use should be clearly communicated.

Expectations for educator, staff, and third-party use should align with **Delphos City Schools** priorities. Educator use

DRAFT

should be in alignment with the Licensure Code of Conduct for Ohio's Educators. Educators and staff must model appropriate acceptable use practices when using AI tools for instructional and operational uses.

Use of tools that have not been approved is not permitted.

All users are expected to employ AI tools solely for educational and related operational purposes, upholding values of respect and academic integrity, and in alignment with other related **Delphos City Schools** policies. Using AI tools for bullying, harassment, and any form of intimidation is strictly prohibited and should be addressed in alignment with existing behavior and discipline policies.

Students and staff with concerns regarding inappropriate use that violates **Delphos City Schools** policies and/or applicable state or federal laws should contact the Superintendent or appropriate designated staff member.

IX. ACADEMIC INTEGRITY

The Board recognizes that the responsible use of AI requires the highest standards of academic integrity with clear expectations for students, educators, and staff regarding the ethical use of AI tools.

AI-enabled tools may be used to support student work (such as brainstorming or feedback), but AI-generated work must not replace student work. Students are expected to complete assignments and assessments in a manner that reflects their own understanding and effort, critically analyze AI-generated content and not misrepresent it as original work, and use proper citations and references for AI-assisted work according to existing policies and expectations relevant to assignments (such as APA or MLA style formats).

The **Delphos City Schools** should specify procedures for investigating and addressing suspected misuse in alignment with existing academic integrity policies.

X. IMPLEMENTATION AND REVIEW

The **Delphos City Schools**, in partnership with the **Delphos City Schools'** ongoing AI workgroup, will monitor developments in AI technology and update policies to address emerging risks. This policy should be reviewed often for effectiveness; alignment to district, school, educator and student needs; considerations of ongoing innovation; related

DRAFT

data privacy and management policies; and impact on students including learning outcomes.

OTHER CONSIDERATIONS

NON-CONSENSUAL INTIMATE IMAGERY

National digital safety experts have emphasized the importance of addressing issues related to Non-Consensual Intimate Imagery (NCII), particularly in terms of local policies on digital wellness and cyberbullying. The Center for Democracy & Technology has created a model policy and related resources that district and schools may want to consider incorporating into relevant local policies. In potential cases where NCII may be used for the purposes of sexual extortion, schools and districts should be aware of Braden's Law and consider how it may apply within existing local policies, as the law classifies sexual extortion as a felony offense in Ohio.

INTEGRATION WITH OTHER RELATED POLICIES

This model policy refers to other existing local policies (such as bullying, academic integrity, and procurement). In addition to cross-references in the required AI-specific policy, districts and schools may want to review and update other related policies to integrate AI as applicable (such as special education policies).

DRAFT