Cyber Threats

Information is everywhere and constantly going from one person to another, from one device to another, etc. By law, some information is protected from disclosure, and, while some information is not technically legally-protected information, it nonetheless has value.

The School adopts this cybersecurity program to safeguards the School's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity, utilizing the best practices for cybersecurity.

Types of Cybersecurity Incident and Ransomware Incident Threats

A "Cybersecurity Incident" is defined as any:

1. Substantial loss of confidentiality, integrity, or availability of the School's information system or network,

2. A serious impact on the safety and resiliency of the School's operational systems and processes,

3. A disruption of the School's ability to engage in business or industrial operations, or deliver goods or services,

4. An unauthorized access to the School's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or a supply chain compromise.

A "Cybersecurity Incident" does not include the mere threat of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity.

"Ransomware Incident" is defined as a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable the School's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

Threats likely to result in Cybersecurity Incidents and Ransomware Incidents most commonly include:

- Data Breach. A leak or spill of sensitive, protected, or confidential data from a secure environment to an insecure environment, where the data may then be copied, transmitted, viewed, stolen, or used in an unauthorized manner. Data breaches often occur with confidential information.

- Denial of Service. Also known as a Distributed Denial of Service ("DDoS") attack, occurs when a server is deliberately overloaded with requests such that the Website shuts down. Users are then unable to access the Website.

- Spoofing/Phishing. Both spoofing and phishing involve the use of fake electronic documents. Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source. Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information (e.g., passwords, credit card numbers, or bank account information) after directing the user to visit a fake website.

    - Spear phishing is a more targeted form of phishing and typically involves sending an email that appears to come from a colleague or acquaintance.

- Malware/Scareware. Illicit software that damages or disables computers or computer systems. Similar to malware is scareware, which uses social engineering to cause fear or anxiety so that a user buys unwanted and unneeded software, such as antivirus software. Computers can become infected through downloading a piece of malware or scareware disguised as legitimate software from peer-to-peer file sharing or email attachments or links. To help prevent malware or scareware, users should keep their software up to date so that any critical software patches are received. Users should also install antivirus software.

    - Ransomware is form of malware in which perpetrators encrypt users' files, then demand the payment of a ransom—typically in virtual currency such as Bitcoin—for the users to regain access to their data. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or images if the victim does not pay. The ransomware is frequently delivered through phishing/spoofing scams.

- Unpatched or Outdated Software Vulnerabilities. Vulnerabilities occur when unpatched or outdated software has not been updated to include the latest software updates allowing unauthorized users to gain access to information networks and systems.

- Removable Media. Media devices that can be connected to computers (e.g. thumb drives, CDs, DVDs, and external hard drives) can be easily stolen, exposing private data. Corrupted devices can be intentionally or unwittingly connected to computers allowing the device to infect the computer with malware.

Staff shall be trained periodically on the School's cyber security procedures, and how to attempt to prevent or mitigate cyber threats and recognize Cybersecurity Incidents and Ransomware Incidents in the event that they may occur.

Types of Security and Preparing for Threats

The School takes a holistic approach to security. There are several security "layers," and each one has its own security strategy as outlined below:

- Physical Security — The security of brick and mortar buildings, as well as the students, faculty, and staff that learn, teach, and work in them..
- Network Security — Focused on ensuring there is not any unauthorized traffic flowing across the network that no one is abusing or gaining illegitimate access to network-connected resources and that sensitive information is security while it is traversing the network (data in motions). DDoS attacks are a form of network resource abuse, and mitigating those attacks is a critical component of network security.
- Application Security — Eliminating software vulnerabilities that could lead to security breaches. The School regularly patches and updates software, applications, and operating systems as recommended by the manufacturers of the products.
- Content Security — Focused on protecting data at rest (e.g., in a database) and on complying with various local, state, and federal requirements for data security and privacy.
- End Point Security — Traditionally concerned with keeping malicious or otherwise unwanted and unauthorized software and users of endpoint devices. This includes asset location tracking and processes for eliminating sensitive data from and reporting lost or stolen devices.
- Cloud/Data Center Security — Focused on ensuring the School's core computing resources are appropriately patched and segmented to prevent unauthorized access and contain any unauthorized access if it does occur.
- Data Backup — To the extent possible, the School maintains offline backups of data or alternative encrypted backups of data.

Staff shall be expected to maintain systems consistent with established security protocols.

Identifying and Reporting an Incident

When a Cybersecurity Incident or Ransomware Incident is suspected, the School's Principal or his/her designee and the School's IT Director should be immediately notified with details regarding the reasons underlying the suspicion and access to the device to the maximum extent possible. The device shall also be taken offline if appropriate.

If a threat is identified to have occurred, the School will implement **Appendix 204.16-A** Cyber Threat Incident Response Plan, to enable the School to focus on containment of the threat.

The Incident Response Team ("IRT"), which shall include the Principal or his or her designee and the IT Director, will work to limit the damage and preserve the protected/sensitive information, and determine the amount of outside external assistance required to assist with addressing the threat.

Any individual whose personal information may have been compromised may also make a report to any of the following:

- FBI, via a Field Office Cyber Task Force;
- Internet Crime Complaint Center;
- National Cyber Investigative Joint Task Force (cywatch@ic.fbi.gov);
- National Cybersecurity and Communications Integration Center (NCCIC@hq.dhs.gov); or
- U.S. Computer Emergency Readiness Team ("US-CERT").

Once the incident has been contained, recovery may be needed for people, policies, and technology—all of which are interconnected. The IRT will need to identify the technology and people impacted by the incident, and address any known causes or existing vulnerabilities.

Payment of Ransomware Incident

In the event the School experiences a Ransomware Incident, the School shall not pay or otherwise comply with a ransom demand unless the Board formally approves the payment or compliance with the ransom demand in a resolution that specifically states why the payment or compliance with the ransom demand is in the best interest of the School.

Notice of Cybersecurity Incident or Ransomware Incident

The School shall notify the following of the Cybersecurity Incident or Ransomware Incident:

- Executive Director of the Division of Homeland Security within the Ohio Department of Public Safety - As soon as possible, but not more than seven days after the discovery of the Cybersecurity Incident or Ransomware Incident

  https://homelandsecurity.ohio.gov/ohio-cyber-integration-center
  OCIC@dps.ohio.gov
  614-387-1089
- Ohio Auditor of State – As soon as possible, but not later than thirty days after the discovery of the Cybersecurity Incident or Ransomware Incident
  Cyber@ohioauditor.gov
  https://ohioauditor.gov/fraud/cybersecurity.html.

R.C. 9.64; **Appendix** Cyber Threat Incident Response Plan.

CERTIFICATION

The Undersigned, being the Board Secretary, hereby certifies that the foregoing represents a true copy of the Board Policy relating to the Prohibition of the Purchase of Certain Food Products policy, as originally adopted by the Board on August 27, 2026, which Policy, is in full force and effect and has not been revoked or amended.

Marquicia Jones-Woods (Sep 4, 2026 08:39:56 EDT)

Marquicia Jones-Woods, Board Secretary

Sep 4, 2026

Date

Cyber Threats Policy

Final Audit Report 2026-09-04

Created:	2026-08-31
By:	Megan Goossen (Megan.Goossen@ideapublicschools.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA0l42glDsOgdVND36W0xugCSnn8d_cEy8

"Cyber Threats Policy" History

Document created by Megan Goossen (Megan.Goossen@ideapublicschools.org)
2026-08-31 - 5:22:56 PM GMT- IP address: 138.43.109.202

Document emailed to qkidzdanceteam@gmail.com for signature
2026-08-31 - 5:46:43 PM GMT

Email viewed by qkidzdanceteam@gmail.com
2026-08-31 - 5:46:49 PM GMT- IP address: 64.233.172.167

Email viewed by qkidzdanceteam@gmail.com
2026-09-04 - 12:35:13 PM GMT- IP address: 66.102.8.36

Signer qkidzdanceteam@gmail.com entered name at signing as Marquicia Jones-Woods
2026-09-04 - 12:39:54 PM GMT- IP address: 172.59.34.29

Document e-signed by Marquicia Jones-Woods (qkidzdanceteam@gmail.com)
Signature Date: 2026-09-04 - 12:39:56 PM GMT - Time Source: server- IP address: 172.59.34.29 - Signature Appearance Selected: MOBILE_DRAW

Agreement completed.
2026-09-04 - 12:39:56 PM GMT