Northside Charter High School
424 Leonard Street, 4th Floor.
Brooklyn, NY 11222

Securing the Future: A Comprehensive Cybersecurity Policy for Nurturing Digital Safety in Educational Landscapes

Introduction

In an age where digital learning is at the heart of education, safeguarding our school's digital domain is paramount. **Northside Charter High School (NCHS)** recognizes the importance of protecting its confidential information, educational resources, and technology infrastructure from cyber threats. This policy outlines the school's commitment to cybersecurity and establishes guidelines for staff, students, and authorized users of NCHS technology. This policy addresses our unwavering commitment to maintaining a resilient digital ecosystem for our students' uninterrupted learning and growth.

Policy brief & purpose

Our school's cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause damage and may jeopardize our school's reputation.

For this reason, NCHS has prepared instructions that may help mitigate security risks. We have outlined the provisions in this policy.

Scope

This policy applies to all our employees, contractors, volunteers, and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

1. Confidential data

We've identified confidential data as our top priority—this includes unpublished financial information, student data, and proprietary educational materials. Our policy provides clear guidelines for protecting personal and company devices, ensuring that all devices are password protected and secured against unauthorized access.

Confidential data is secret and valuable. Examples are:

- Unpublished financial information
- Data of students (Historical Data, Current Enrollment Data and other prospective data for the students)
- New technologies, lesson plans, grades, SIS credentials, and other academic platforms secured through various security policies such as SSO and other security measures.

2. Everyone at NCHS is required to safeguard this data

Furthermore, to enhance our staff's ability to recognize and respond to cybersecurity threats through comprehensive training modules prepared by NCHS with our vendors and partners. These include essential programs on internet security, social engineering red flags, and common threats, all aimed at fostering a vigilant and informed school community. (Best Practices Guideline for Staff & Students')

3. Implementation Strategies

Our approach to practical implementation involves a mandatory completion timeline for all staff training **before commencement of the next school year,** regular application of training insights, and a commitment to continuous improvement. Our policy also includes a **bi-annual review** schedule to adapt to evolving cybersecurity landscapes and detailed incident response plans to efficiently manage potential cybersecurity incidents.

4. Technology Security

The NCHS commits to maintaining secure network systems, including the protection of all personally identifiable information, adhering to federal and state privacy and data governance laws such as FERPA.

Practical Implementation:

- **Completion Timeline:** Mandatory completion of training programs within the third quarter of 2024.
- **Application and Awareness:** Integration of training insights into daily operations, supported by ongoing discussions and simulations.

Regular Policy Review and Updates:

- **Bi-annual Review Schedule:** To adapt to evolving cybersecurity landscapes, incorporating feedback from IT staff, administrative members, and external consultants.
- **Continuous Improvement:** Training outcomes will inform updates to our cybersecurity practices and policy.

Detailed Incident Response Plan

Develop a comprehensive plan detailing roles, responsibilities, and procedures for various cybersecurity incidents, complemented by semi-annual drills.(For DRP Policy Document Click here)

Third-Party and Vendor Management

Formalize a vetting process for third-party vendors, ensuring compliance with our cybersecurity standards and incorporating data protection clauses in agreements. (For 3rd Party Vendor Management Policy Click here)

Additional Policy Enhancements

1. **Cyber Ethics:** Integration of cyber ethics into the curriculum and staff training.
2. **Student and Parent Engagement:** Offering informational sessions and resources on cybersecurity.
3. **Cybersecurity Risk Assessment:** Annual assessments to identify and mitigate potential vulnerabilities.
4. **Physical Security Measures:** Strengthening physical security protocols for IT infrastructure.
5. **Compliance with Additional Regulations:** Ensuring adherence to relevant local, state, or federal regulations.

Enhancements and Engagements

NCHS incorporated additional policy enhancements, emphasizing cyber ethics, student and parent engagement, and stringent physical security measures. Furthermore, we recognize the importance of compliance with additional regulations and the strategic use of encrypted connections for remote access to our school network.

NCHS mandate all employees to comply with our internet usage policy.

Our IT Specialists Team:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange security training for all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow the cyber security policies provisions as other employees do.

Reactionary cyber plan

If the system is breached the following action plan is initiated:

a) First: Physically lock down and determine all the device(s) or computer that has been infiltrated. Do not allow staff that is not IT personnel or higher to access the device. Change passwords associated with infected accounts, computers, and anything else that is associated. Disconnect device(s) from the network through the remote desktop in the IT Office to avoid spreading.

b) Second: Contact Atlantic to discuss what was taken or lost from the computer. **(Atlantic's contact number: 212-741-6400 ext 2408)**
c) Third: Contact Beazley for forensics, legal, and public crisis management. Discussion of losses, causes, and recovery options. We will then proceed with their own breach response that is outlined in the contract.
(Beazley contact number: 866-567-8570)
d) Fourth: After forensics and vulnerability patches, the affected devices will be wiped and factory reset regardless of what information is on the device prior to being reintroduced to the company's private network, unless advised otherwise by Atlantic, Beazley, or the Administrator team at Northside Charter.

The policy ensures a proactive and educated approach to cybersecurity, involving all stakeholders in the district's digital ecosystem.

Continuous Engagement and Improvement

Feedback Loop: Establish mechanisms for collecting feedback on cybersecurity practices from staff, students, and parents, facilitating continuous improvement.

Policy Updates: Regular updates to the policy will reflect technological advancements, emerging threats, and changes in regulatory requirements.

Physical and Digital Security Integration

- Ensure a holistic approach to security that encompasses both physical and digital measures, recognizing the interconnectivity between the two in protecting sensitive information and technology assets.

Compliance and Legal Obligations

- Stay abreast of and ensure compliance with all relevant cybersecurity laws and regulations, conducting regular reviews to align policy and practices with legal obligations.

Strategic Partnerships and Resources

- Leverage partnerships with vendors like Atlantic, and other educational institutions to share knowledge, resources, and best practices in cybersecurity.
- Utilize available technologies and services that enhance the NCHS cybersecurity posture and compliance capabilities.

Incident Response and Recovery

- Establish clear protocols for incident response, including immediate actions, reporting procedures, and recovery plans, ensuring minimal impact and swift return to normal operations.
- Regularly test and refine the incident response plan through drills and simulations, incorporating lessons learned into policy and training updates.

Engagement with Law Enforcement and Regulatory Bodies

- Develop protocols for engaging with law enforcement and regulatory bodies in the event of significant cybersecurity incidents, ensuring compliance with legal requirements and facilitating effective incident resolution.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee in security.
- Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Take security seriously.

Everyone, from our students and parents to our employees and vendors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Conclusion

This comprehensive cybersecurity policy, enhanced by targeted training initiatives and strategic policy enhancements, positions the school as a proactive entity in the realm of digital security. By adopting a holistic and adaptive approach to cybersecurity, the district not only protects its technological assets but also fosters an environment of awareness, responsibility, and resilience among its students, staff, and broader community. The commitment to ongoing review, stakeholder engagement, and adherence to legal obligations underscores the district's dedication to maintaining a secure and trustworthy digital learning environment.