Beverly Hills International School

Cybersecurity Policy

Table of Contents

1- Beverly Hills International School Mission and Vision:

Mission:

Our mission is to deliver exceptional education to all students and the community, while fostering citizenship, ethical values, and social responsibility.

Vision:

Our vision is to nurture a generation that is creative, caring, and proud of its heritage. We strive to provide an inspiring environment that fosters critical thinking, creativity, empowerment, and the achievement of personal and academic excellence.

2- Purpose

This policy aims to establish robust measures to safeguard the digital infrastructure, systems, and data of Beverly Hills International School ensuring the privacy and security of students, staff, and stakeholders.

3- Scope

This policy applies to all members of the school community, including students, teachers, administrative staff, contractors, and any individuals accessing the school's digital resources or networks.

4- Objectives

- Protect sensitive information, including student records, staff data, and other confidential materials.
- Prevent unauthorized access, data breaches, and cyber threats.
- Promote responsible use of digital resources across the school.

5- Key Components of the Policy

a. Access Control

- Ensure that access to school systems and data is role-based and limited to authorized personnel.
- Implement strong password policies, requiring complex passwords and periodic password updates.

b. Data Protection and Privacy

- Encrypt sensitive data stored on school servers or transmitted over networks.
- Maintain secure backups of all critical data and review backup integrity regularly.
- Comply with data protection laws and regulations (e.g., GDPR, FERPA, or local regulations).

c. Internet and Network Security

- Secure the school's Wi-Fi with strong encryption (e.g., WPA3) and a unique password.

- Separate guest and internal networks to limit vulnerabilities.
- Monitor network traffic regularly to identify and mitigate threats.

d. Device Security

- Install and update antivirus software on all school-owned devices.
- Ensure timely updates and patching of all software, operating systems, and applications.
- Prohibit the use of personal devices for accessing sensitive school data without prior authorization.

e. Email and Communication Security

- Provide email filtering systems to detect and block phishing, spam, and malicious content.
- Educate staff and students about recognizing phishing attempts and suspicious links.
- Enforce policies regarding the secure sharing of sensitive information via email.

f. Cybersecurity Awareness and Training

- Conduct mandatory training sessions on cybersecurity best practices for all staff and students.
- Regularly update the community about emerging cybersecurity threats and prevention methods.

g. Incident Response Plan

- Develop a clear procedure for reporting cybersecurity incidents, including a dedicated point of contact.
- Establish steps for responding to data breaches or cyber-attacks, including containment, investigation, and recovery.
- Document and analyze incidents to prevent future occurrences.

6- Responsibilities

- **IT Department:** Ensure the implementation and maintenance of cybersecurity systems and protocols.
- **School Leadership:** Oversee cybersecurity compliance and allocate necessary resources.

- **Staff and Students:** Adhere to all cybersecurity guidelines and report potential threats promptly.

7- Enforcement

Non-compliance with the cybersecurity policy may result in disciplinary actions, including restricted access to school systems or other measures based on the severity of the violation.

8- Policy Review and Updates

This policy will be reviewed annually to address new cybersecurity challenges, technologies, and regulations.