Staff Technology Acceptable Use and Safety Board Policy

The Board provides Technology and Information Resources to support the educational and professional needs of staff and students. This policy governs the use of District technology resources, including computers, networks, and Internet access. It aims to promote educational excellence while ensuring responsible and safe use of these resources. The policy outlines expectations, restrictions, and consequences related to technology use in the educational environment.

Reference SDH Board Policy po7540.04

Purpose and Scope of Technology Resources

1 Limited Educational Purpose

The District's computer network and Internet system are provided for limited educational purposes only, not as a public access service or forum.

2 Regulated Use

Use of District Technology and Information Resources is governed by principles consistent with applicable laws and the District's educational mission.

3 No Privacy Expectation

Users have no right or expectation to privacy when using District Technology and Information Resources.

4 Resource Preservation

Restrictions are in place to preserve limited resources such as bandwidth, storage space, and printers.

Internet Access and Safety Measures

1

Technology Protection Measures

The Board has implemented measures to protect against access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors.

2

Monitoring Online Activity

Software and/or hardware is utilized to monitor online activity of staff members and block/filter access to inappropriate content.

3

Unblocking Appropriate Content

The District Administrator or designee may temporarily or permanently unblock access to websites containing appropriate material if inappropriately blocked.

Staff Professional Development

Safety and Security

Training on the safety and security of students while using e-mail, chat, social networking, and other forms of direct electronic communications.

Online Dangers

Education on the inherent danger of students disclosing personally identifiable information online and the consequences of unauthorized access.

Cyberbullying Awareness

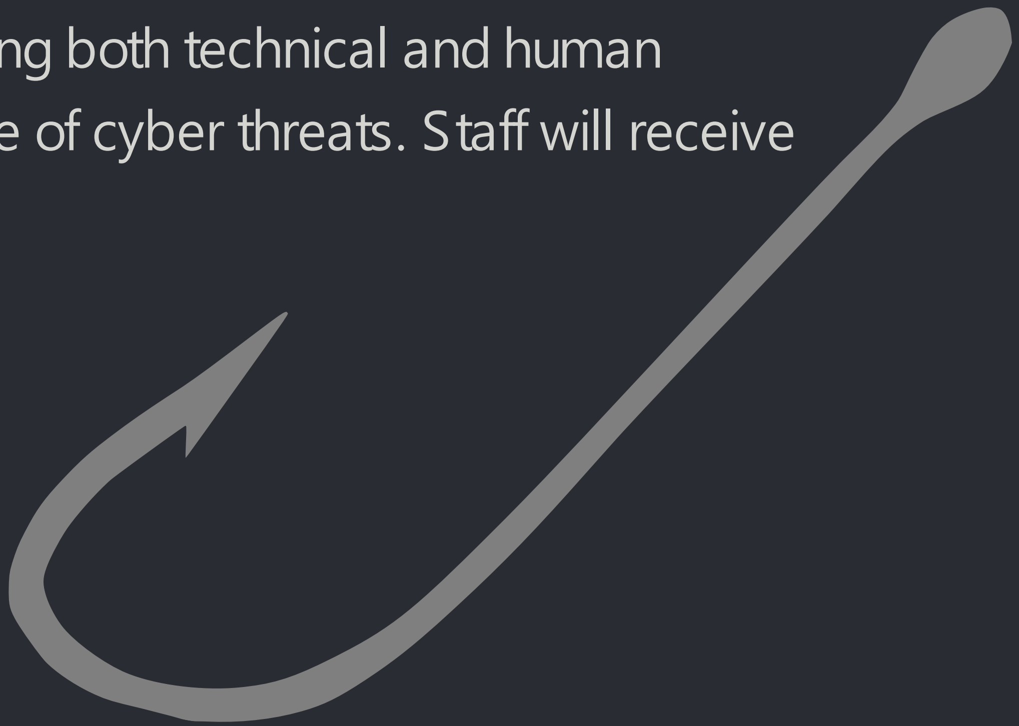
Instruction on cyberbullying awareness and response, as well as other unlawful or inappropriate online activities.

Information Security

Information Security refers to the practices and measures taken to protect digital information and systems from unauthorized access, damage, or disruption. This includes safeguarding against cybersecurity threats like phishing attacks.

Phishing is a type of social engineering attack where hackers attempt to trick users into revealing sensitive information, such as login credentials or financial data, often through deceptive emails or websites. Effective cybersecurity strategies involve educating users on how to identify and avoid phishing attempts.

The District will provide security awareness training for employees. By addressing both technical and human vulnerabilities, organizations can better protect themselves against a wide range of cyber threats. Staff will receive opportunities via email throughout the year.



Staff Responsibilities

1

Provide Instruction

Staff members shall provide instruction for their students regarding appropriate technology use, online safety, and security.

2

Monitor Activities

Staff will monitor students' online activities while at school, including visual observations and use of specific monitoring tools.

3

Protect Student Privacy

The disclosure of personally identifiable information about students online is prohibited.

Email and Online Services

School Email Addresses

Staff will be assigned a school email address for professional communication.

Student Accounts

With prior approval, staff may direct students to use school-assigned email accounts for registering for educational services. Requests for students to use web resources that require accounts may be submitted via online form on the District website.

Policy Acknowledgment

Staff and Board members using the District's e-mail system shall acknowledge their review of and intent to comply with the acceptable use policy.

Social Media and Personal Use

Unintended Consequences

An employee's personal or private use of social media may have unintended consequences that could compromise the District's mission or cause disruption.

First Amendment Rights

While the Board respects employees' First Amendment rights, these do not include permission to post inflammatory comments.

Professional Responsibility

Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

Reminders

The District takes violations of this technology policy very seriously. Users are personally responsible and liable, both civilly and criminally, for any unauthorized uses of District technology and information resources. Violators may face serious consequences, including suspension or revocation of their access privileges, as well as potential disciplinary action.

Credit: Slides and images made with Gamma.