Blanket ISD Acceptable Use Policy (AUP)

I. Introduction

Each employee, student or non-student user of Blanket Independent School District (BISD) information system is expected to be familiar with and follow the expectations and requirements of this administrative rule. The purpose of this rule is to ensure that individuals are aware of their responsibilities regarding the Internet and related technology and equipment. This rule also helps ensure the safety and privacy of current and former employees and students.

A. Legal Requirements

BISD is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

1. The Family Educational Rights and Privacy Act (FERPA)
2. Children's Internet Protection Act (CIPA)
3. Children's Online Privacy Protection Act (COPPA)

Users of BISD's network are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies through the use of BISD networks may result in discipline or litigation against the offender(s) by the proper authority. BISD will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

B. Acceptable Use

BISD provides computer, network, e-mail, and Internet access to individuals as part of the learning environment. The use of these resources is a privilege and not a right. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use by every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline or litigation in accordance with board policy and state and federal law.

II. Employee Acceptable Use

This section is dedicated to provide BISD employees with guidance of acceptable use of the District's information technology resources, including but not limited to:

1. The internet, intranet, e-mail, portal
2. District assigned computing devices such as personal electronic devices, laptops and desktops and

3. The District's network and supporting systems and data transmitted by and stored on the BISD systems.

A. Annual Responsibilities and Information Security Awareness

Staff members will review the Information Security Awareness materials presented on the BISD website annually.

B. Prohibited Use of BISD Resources

The following uses of BISD computer resources by staff members are prohibited at all times:

1. Unauthorized or excessive personal use. Any personal use should not interfere with or impair an employee's job performance.
2. Infringing upon the intellectual property rights of others or violating copyright laws.
3. Uploading or transferring out of the District's direct control any software licensed to the District or data owned by the District without explicit written authorization. Failure to observe copyright or license agreements can result in disciplinary action from BISD or legal action by the copyright owner.
4. Unauthorized use of resources (including but not limited to servers, networks, computers and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms.
5. Bypassing or attempting to bypass any of the District's security or content filtering safeguards.
6. Granting another individual access to any District accounts that have been authorized to you or using another individual's District authorized accounts, user-id's and/or passwords.
7. Allowing another person to use a District system under his or her login.
8. The use of any "hacking tools" that can be used for gaining unapproved access on any device may not be possessed on school property, on any District premise, or run or loaded on any District system.
9. Violating any state or federal law or regulation, board policy or administrative rule.

C. Sensitive Information

BISD employees who have or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and other applicable laws and regulations, as they relate to the release of student information.

1. Employees may not disclose sensitive or personally identifiable information regarding students to individuals and/or parties not authorized to receive it. Authorization to

disclose information of a student to individuals and/or parties must strictly adhere to regulations set forth in the FERPA - See Board Policy and Administrative Rule JR.
2. Information contained in these records must be securely handled and stored according to BISD directives, rules and policies and if necessary destroyed in accordance with state information retention standards and archival policy.

D. Limited Personal Use

BISD does not grant any ownership, privacy or an expectation of privacy in the contents of any message, including email, or other Internet activities involving BISD resources or equipment.

Personal use of Blanket ISD technology is prohibited if:

1. It interferes with the use of IT resources by the District;
2. Such use burdens the District with additional costs;
3. Such use interferes with the staff member's employment duties or other obligations to the District; or
4. Such use includes any activity that is prohibited under any district (including this rule), board policy, or state or federal law.

Each District e-mail user is responsible for the content of all text, audio, or image that he or she places or sends over the Internet or District email systems.

- Email messages are considered public records and may be released pursuant to the requirements of the Texas Freedom of Information Act.

E. Consequences

Employees who violate this administrative rule may be subject to discipline, including up to termination. All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to the School Principal or Superintendent. Suspected criminal activity must be immediately reported to law enforcement.

III. Student Acceptable Use

This section is dedicated to provide BISD students with guidance of acceptable use of the district's information technology resources, including but not limited to:

1. The internet, intranet, e-mail, portal;
2. District assigned computing devices such as personal electronic devices, laptops, desktops and portable storage; and
3. The District's network and supporting systems and data transmitted by and stored on these systems.

A. Compliance with Copyright Laws

Students are to follow copyright laws at all times. Students should refer all questions regarding copyright concerns to administrators at their school.

B. Filtering and Monitoring Computer Resources

The District takes reasonable precautions by using filtering software to keep inappropriate Internet sites and e-mail out of the classroom. The District strongly adheres to the guidelines set forth by COPPA and CIPA when installing filtering/monitoring software devices on District equipment. The District does not supervise individual e-mail accounts.

1. The District reserves the right to review any e-mail sent or received using District equipment and e-mail accounts.
2. Students must adhere to the behavior expectations while using technology and e-mail, including but not limited to those expectations contained in board policy. The District's Student Code of Conduct is updated every year and available via the District website.
3. Technology is constantly changing and evolving. Due to the nature of the Internet, online communications, and evolving technology, the District cannot ensure or guarantee the absolute safety of students during the use of technology, including email and the Internet. Parents and students should contact the school immediately with any concerns related to the use of technology.

C. Prohibited Uses of BISD Resources

The following uses of BISD computer resources by students are prohibited from:

1. The use of obscene, bullying, profane, lewd, threatening, disrespectful, or gang related language or symbols.
2. The bypass or attempt to bypass any of the District's security or content filtering safeguards.
3. Allowing another person to use the computer under your District login.
4. Adding, modifying, repairing, reconfiguring or otherwise tampering with any device on the network infrastructure including, but not limited to: wireless network devices, computers, printers, servers, cabling, switches/hubs, routers, etc.
5. Unauthorized access, overloading, more commonly known as Distributed Denial of Service or Denial of Service, or use, or attempted unauthorized access or use of District information systems.
6. Destroying or tampering with any computer equipment or software.
7. The use of any "hacking tools" that can be used for gaining unapproved access on any device may not be possessed on school property, on any District premise, or run or loaded on any District system.
8. The use of school computers for illegal activities including but not limited to planting viruses, hacking, or attempted unauthorized access to any system.

9. Violating any state or federal law or regulation, board policy or administrative rule.

D. Agreement of Use

Students, parents, and guardians agree that BISD computer equipment must be handled with care and respect.

E. Consequences

Students who violate this administrative rule may be subject to disciplinary action in accordance with board policy and state and federal law. Suspected criminal activity must be immediately reported to law enforcement.

IV. BISD Internet Safety and Other Terms of Use

A. General Access

In compliance with the Children's Internet Protection Act ("CIPA"), U.S.C. §254 (h), the District uses technological devices designed to filter and block the use of any of the District's computers with Internet access to retrieve or transmit any visual depictions that are categorized as obscene, child pornography, or "harmful to minors" as defined in the CIPA.

1. Though the District makes reasonable efforts to filter such Internet content, the District cannot warrant the effectiveness of its Internet filtering due to the dynamic nature of the Internet.
2. Users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled to conduct bona fide research for another lawful purpose. These requests should be made to the Technology Coordinator with the knowledge of that employee's supervisor.

B. Education, Supervision, and Monitoring

It shall be the responsibility of all District school staff to make a reasonable effort to educate, supervise, and monitor appropriate usage of online computer network access to the Internet in accordance with this administrative rule, CIPA, COPPA, and the Protecting Children in the 21st Century Act.

C. Personal Safety

The following list is considered precautions taken by BISD to ensure the safety of their students, employees, and other individuals.

1. Students will not post or email personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication.

2. Students will not agree to meet with someone they have met online without their parent/guardian's approval.
3. Students will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
4. Employees will report any concerns related to their use of technology to their immediate supervisor.

D. Expectation of Privacy

Individuals should not have an expectation of privacy in the use of the District's email, systems, or equipment. The District may, for a legitimate reason, perform the following:

1. Obtain emails sent or received on District email.
2. Monitor an individual's use on the District's systems.
3. Confiscate and/or search District-owned software or equipment.

The District may confiscate and search personal electronic devices in accordance with Texas Law.