PROMISE ACADEMY
("School")

Acceptable Use Policy for School Computer Systems

INFORMATION FOR EMPLOYEES

I. OBJECTIVES

The School's Acceptable Use Policy ("Policy") has been developed to ensure security and reliability of our systems and network and the networks and systems of others, prevent unauthorized access and other unlawful activities by users online, and to prevent unauthorized disclosure of or access to sensitive information.

The School will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network, as required by the Children's Internet Protection Act ("CIPA").

A. Student Internet Safety

1. Students under the age of eighteen should only access School accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use;

2. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students may not reveal their name, home address, telephone number, or display photographs of themselves or others;

3. Students shall not meet in person anyone they have met only on the Internet; and

4. Students must abide by all laws, this Acceptable Use Policy, and School security policies.

The School reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of School property, network, and/or Internet access or files, including email.
As used in this Policy, "user" includes anyone using the computers, Internet, email, chat rooms, and other forms of direct electronic communications or equipment provided by the School ("Network"). Only current students or employees are authorized to use the network. Employees' use of the Network is limited to legitimate educational purposes, incident to their assignments, work responsibilities, and independent research related to their assignment.

II. ACKNOWLEDGEMENT OF POLICY

The School must verify that each employee using the computer network and Internet access has a signed page acknowledging this Policy. The signed acknowledgment page remains in effect until revoked, or the employee loses the privilege of using the School's network due to violation of this Policy, or is no longer a School employee. Employees and other users are required to follow this Policy. Even without signature, all users must follow this Policy and report any misuse of the network or Internet to a supervisor or other appropriate School personnel. Access is provided primarily for education and School business. By using the network, users have agreed to this Policy.

If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a supervisor or other appropriate School personnel.

III. UNACCEPTABLE USES OF THE COMPUTER NETWORK OR INTERNET

A. Transmitting on or through the network any material that is, in the School's sole discretion, unlawful, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise

violate any local, state, national or international law, statute or regulation.

B. Accessing or transmitting pornography of any kind, obscene depictions, harmful or offensive materials, materials that encourage others to violate the law, confidential information, or copyrighted materials;

C. Selling or purchasing illegal items or substances;

D. Using non-School email websites, spreading SPAM (unsolicited email), “chain letters,” or viruses;

E. Causing harm to others or damage to their property, such as:

1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others;

2. Deleting, copying, modifying, or forging other users’ names, emails, files, or data; disguising one’s identity, impersonating other users, or sending anonymous email;

3. Disrupting services, destroying data, destroying or damaging equipment, or disrupting the operation of the network in any way, including the intentional distribution or posting of any virus, worm, Trojan horse, or computer code intended to cause harm;

F. Users may not attempt to circumvent user authentication or security of or jeopardize access to any host, network, or account. This includes, but is not limited to:

1. Accessing data the user is not expressly authorized to access;

2. Probing the security of the School’s network and the networks of others, password sniffing, IP spoofing;

3. Using another’s account password(s) or identifier(s);

4. Interfering with other users’ ability to access their account(s); or

5. Disclosing anyone’s password to others or allowing them to use another’s account(s).

6. The use of annonymizers (using a web site to bypass the School’s filtering system) is not allowed.

G. Using the network or Internet for Commercial purposes:

1. Using the Internet for personal advertising, promotion, or financial gain; or;

2. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.
Employees should model the behavior expected of students and not access entertainment sites, such as social networking or gaming sites, except for legitimate educational purposes.

IV. PENALTIES FOR IMPROPER USE

The use of the School network is a privilege, not a right, and misuse will result in the restriction or cancellation of the use. The administrator, supervisor, or systems administrator may limit, suspend, or revoke access to the network at any time. Misuse may also lead to disciplinary and/or legal action for employees, including suspension, dismissal from School employment, or criminal prosecution by government authorities. The School will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

V. CONFIDENTIALITY

Users with access to confidential data are to utilize all appropriate precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur.

VI. DISCLAIMER

The School makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations that result or have alleged to have resulted from the use of or inability to use the network; or that results from mistakes, omissions, interruptions, deletion of files, loss of data, errors, defects, delays in operations, or transmission or any failure of performance, communications failure, theft, destruction or unauthorized access to the School's records, programs, or services. The School further denies any responsibility for the accuracy or quality of information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the School, its affiliates, or employees.

VII. RETENTION OF SCHOOL AND PUPIL RECORDS

Information generated or stored on the network, including but not limited to e-mail, e-mail attachments, web postings, and voice mail messages may constitute pupil records or School records. Employees shall ensure that pupil and School records are retained as set forth below.

School e-mail accounts are not intended for permanent storage of e-mail. The School may retain or dispose of an employee's email, whether an employee is currently or formerly employed by the School. All email folders may be purged as often as every 90 days by the School's information technology department. E-mail trash folders may be purged as often as every 30 days by the School's information technology department.
Each employee is responsible for retaining School records and pupil records, as defined below, that he or she generates on the network, including but not limited to e-mail, by doing at least one of the following:
1) saving the record to an electronic system other than the School e-mail account;
2) electronically archiving the document; or
3) printing the document on paper and appropriately filing the printed document.

School and pupil records shall be maintained until such time as the director/principal or designee designates the records as disposable records and orders their destruction pursuant to applicable laws.

School records include all records, maps, books, papers, and documents (including e-mail) of the School required by law to be prepared or retained or which are prepared or retained as necessary or convenient to the discharge of official duty. Employees are advised that many School records also constitute public records disclosable to members of the public upon request.

Pupil records include any item of information directly related to an identifiable pupil, other than directory information, which is maintained by the School or required to be maintained by an employee in the performance of his or her duties, whether recorded by handwriting, print, tapes, film, microfilm, or other means, such as electronic mail. Pupil records do not include informal notes related to a pupil compiled by a school officer or employee which remains in the sole possession of the maker and are not accessible or revealed to any other person except a substitute.

I have read, understand, and agree to abide by the provisions of the Acceptable Use and Security Policies of the School.

_____
Employee Name (Print)

_____
Employee Signature Date

Please return this form to the school or office where it will be kept on file. It is required for all employees that will be using a computer network and/or Internet access.