ZALMA R-V SCHOOL DISTRICT'S ACCEPTABLE USE AGREEMENT

Internet Safety Policy

A. Introduction

It is the policy of the Zalma R-V School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act.

B. Access to Inappropriate Material

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

C. Internet Safety Training

In compliance with the Children's Internet Protection Act, each year, all District students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying and cyberstalking awareness and response.

D. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chatrooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking", and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

E. Supervision and Monitoring

It shall be the responsibility of all District employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the District's Technology Department under the sole authority and decision of the District's administrators.

Internet Usage

A. Personal Responsibility

Access to electronic research requires students and employees to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations Policy as well as employee handbooks clearly apply to students and employees conducting electronic research and communication.

One fundament need for acceptable student and employee use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases files, and information banks. Personal passwords/account codes may be created to protect students and employees utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students or employees use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal laws. Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.

B. **Acceptable Use**

The use of the District technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities which are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses/malware or harmful programs on, or through the computer system; unauthorized downloads or installation of any program; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the Internet; using personal electronic communications and/or accounts; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment. Students or employees may not use copyrighted materials without the permission of the copyright holder. The Internet allows access to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (E-Mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-Mail system is designed solely for educational and work related purposes. E-mail and computer system files are subject to review by District and school personnel at any time. Chain letters, "chat room" or Multiple User Dimensions (MUDs) are not allowed, with the possible exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

Students or employees who engage in "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may be describes as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter" which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions. Similarly, the use of any District computer to access sites which allow the user to conceal their objective of accessing inappropriate material is not permitted.

The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

C. **Internet Access**

In compliance with the Children's Internet Protection Act (CIPA), the District uses technological devices designed to filter and block the use of any District computer with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography, or "harmful to minors" as defined by CIPA and material which is otherwise inappropriate for District students.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that do not fall into these categories are blocked by the filter. In the event that a District student or employee feels that a website or web content has been improperly blocked by the District's filter and this website or web content is appropriate for access by District students, the process described below should be followed:

1. Follow the process prompted by the District's filtering software and submit an electronic request for access to a website, or:
2. Submit a request, to the District's Principal and Superintendent.
3. Requests for access shall be granted or denied within three days.
4. Appeal of the decision to grant or deny access to a website is to be made in writing stating detailed reasons for the grant or deny access to a website to the Board of Education for review at their next monthly meeting.
5. In case of an appeal, the Board of Education will review the contested material and make a determination.
6. Material subject to the complaint will not be unblocked pending this review process.

D. **Privileges**

The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of privileges. All staff members and students who receive a password/account code will participate in an orientation or training course regarding the proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

E. **Network Etiquette and Privacy**

Students and employees are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

1. System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others. Cyberbullying and Cyberstalking are prohibited at all times.
2. System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.
3. System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during E-Mail transmissions.
4. System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users. Inserting personal devices into the District technologies is prohibited at all times.
5. System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The District technology department and administrators may access and read E-mail and District computer systems on a random basis.
6. Use of the District's electronic network for unlawful or personal purposes will not be tolerated and is prohibited.
7. **System users are not allowed to delete any browser history**.

F. **Services**

While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

G. **Security**

The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher, technology department, or an administrator.

The District shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA), and the Neighborhood Internet Protection Act (NCIPA).

H. **Vandalism of the Electronic Network or Technology System**

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District Information service, or the other networks and equipment that are connected to the Internet. This includes, but is not limited to the uploading or the creation of computer viruses/malware, the alteration of data, or the theft of restricted information or any technology equipment. Any vandalism of the District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

I. Wi Fi Capabilities

In the event when Wi Fi Capabilities become available for students and staff, the following will apply:

1. **Staff may utilize Wi Fi during their planning period and before or after school only.**
2. **Students may utilize Wi Fi on their personal devices during school hours for school work only. They may have access before and after school and during lunch for personal activities as long as they adhere to the network and etiquette privacy rules.**

J. Consequences

The consequences for violating the District's Acceptable Use Policy include, but are not limited to, one or more of the following:

1. Suspension of District Network privileges;
2. Revocation of Network privileges;
3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;
8. Expulsion; or
9. Employee disciplinary action up to and including dismissal.

ZALMA R-V SCHOOL DISTRICT'S ACCEPTABLE USE AGREEMENT

Please keep pages 1-4 for your future reference, and please return this signed form to the school where it will be kept on file.

I have read, understand, and agree to abide by the provisions of the Zalma R-V School District's Acceptable Use Policy.

STUDENTS AND PARENTS/GUARDIANS SIGNATURE:

DATE: _____

GRADE: _____

STUDENT SIGNATURE: _____

STUDENT PRINT NAME: _____

DATE: _____

PARENT/GUARDIAN SIGNATURE: _____

PARENT/GUARDIAN PRINT NAME: _____

COMMUNITY MEMBER SIGNATURE:

DATE: _____

COMMUNITY MEMBER SIGNATURE: _____

COMMUNITY MEMBER PRINT NAME: _____

STAFF MEMBER SIGNATURE:

DATE: _____

STAFF SIGNATURE: _____

STAFF PRINT NAME: _____