PALMYRA AREA SCHOOL DISTRICT
Responsible Use of Internet and Network Resources Procedures
Internet, E-mail and Network Access Agreement
All District Users

Purpose:
The Palmyra Area School District supports the use of the Internet and other technological resources in the district's instructional and operational programs in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

Procedures:
Palmyra School District reserves the right to log and monitor Internet use, computer network activity, and fileserver space utilization by district users. Network storage areas may be treated like school lockers. Network administrators, school administrator & / or faculty may review student and staff files and communications to maintain system integrity and ensure that students and staff are using the system responsibly. Users should not expect that files stored on district servers or computers will be private. Palmyra School District reserves the right to remove a user account from the network to prevent further unauthorized or illegal activity. Palmyra School District reserves the right to log and monitor E-mail. Staff will educate students about appropriate online behavior including interacting with others on social networking websites and chat rooms and cyber bullying awareness and response.

Students and staff must sign the Responsible Use Agreement in order to have E-mail, Internet access, and access to the network. All signed permission forms will be kept on file.

Responsible Use Policy:
Students and staff are expected to act in a responsible, ethical, and legal manner in accordance with district policy, professional code of conduct, accepted use network etiquette, and federal and state law. Use of the Internet, E-mail and network technology must be in support of the educational mission and instructional program of the School District. Students and staff bear the burden of responsibility to inquire with administration, the Technology Department, or teachers when they are unsure of the permissibility of a particular use of technology prior to engaging in use. With respect to all users, the following are prohibited.

1. Use for inappropriate or illegal purposes and activity.
2. Use for commercial, private advertisement or for-profit purposes.
3. Use for lobbying or political purposes.
4. Use to infiltrate or interfere with a computer system and/or damage the data, files, operations, software, or hardware components of a computer or system.
5. Hate mail, harassment, discriminatory remarks, threatening statements and other inflammatory communication.
6. The unauthorized or illegal installation, distribution, reproduction or use of copyrighted software.
7. Use to access, view, or obtain material that is obscene, pornographic or child pornography or is deemed harmful and inappropriate for minors.
8. Use to transmit material likely to be offensive or objectionable to recipients.
9. Impersonation of another user or anonymity. Use to obtain, copy or modify files, passwords, data or information belonging to other users.
10. Intentional obtaining or modifying of e-mail, files, passwords, and data belonging to other users.
11. Loading or use of unauthorized games, programs, files, music or other electronic media.
12. Use to disrupt the work of other persons (the hardware or software of other persons shall not be destroyed, modified or abused in any way).
13. Attempting to circumvent any security system or filter employed by the district, including the use of websites or proxy servers to tunnel around firewalls and filtering software, or utilizing the district network or Internet to circumvent any school policy. The Filter may be disabled by the network administrator or faculty with appropriate access credentials at the workstation level for use by an adult administrator or teacher for bona fide research or other lawful purposes. The Filter may not be disabled for use by students or other minors for any reason.
14. Use to upload, create or attempt to create a computer virus.
15. The unauthorized disclosure, use or dissemination of personal information regarding minors.
16. Inappropriate language and profanity.
17. Bullying, cyber bullying, or harassment.
18. Fraudulent copying, communications, or modification or materials in violation of copyright laws.
19. Posting of someone else's intellectual property, including but not limited to text, photographs, and video; this includes intellectual property that the user was given permission to use personally, but not publicly.

Consequences / Disciplinary Action for Inappropriate Use By Staff:

Failure to follow the procedures and prohibitions listed above may result in the loss of the right of access to network resources. Other appropriate staff disciplinary procedures may take place including, but not limited to, a written reprimand, unsatisfactory rating and / or possible termination, as needed. The severity of the infraction will determine the appropriate disciplinary action.

Illegal use of the network, intentional deletion or damage to files or data belonging to others, copyright violations, or theft of services may be reported to the appropriate legal authorities for possible prosecution.

Employee Name (Print) _____ Date _____

Employee Signature _____ Date _____