Newcastle. Independent School District
Acceptable Use and Internet Safety Policy

The Newcastle ISD system will be used only for administrative and educational purposes consistent with the Newcastle ISD mission and goals. Commercial use of the system is strictly prohibited.

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes

The district will provide training to employees in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the Newcastle ISD system will emphasize the ethical use of this resource.

The Technology Coordinator will be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.

The Technology Coordinator will ensure that all users of the District's system complete and sign annually an agreement to abide by District policies and administration of the system.

Consent Requirements

Copyrighted software or data may not be placed on any system connected to the Newcastle ISD system without permission from the holder of the copyright. Only the owner(s) or individuals the owner specifically authorized may upload copyrighted material to the system.

No original work created by the District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor)

No personally identifiable information about a District student will be posted on a Web page under the District's control unless District has received written consent from the student's parent. The Family Educational Rights and Privacy Act and District policy may make an exception for "directory information" as allowed.

Filtering

All Internet access will be filtered for minors and adults on computers with Internet access provided by the school. The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of

violence, illegal use of weapons, drug use, discrimination, or participation in hate groups, instructions for performing criminal acts (e.g., bomb making); and on-line gambling. Any site with visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as deemed by the federal Children's Internet Protection Act and as determined by the Superintendent will be blocked.

System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

The student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

Filtering for the Newcastle ISD will be done under an agreement with Region IX Education Service Center using Web Sense. In the event that a student accesses an unacceptable site, a request will be e-mailed to Acnet, who facilitated the Web Sense Filter. The site will be blocked upon receipt of the e-mail.

Requests to Disable Filter

The filter can be disabled for sites needed for bona fide research or other lawful purposes. The unblocking of each site must be a request from a teacher supervising the research or study unit. The Technology Director must approve the request and the director will be responsible for disabling the filter.

System Access

Access to the District's electronic communications system, including the Internet, shall be made available
to students and employees primarily for instructional and administrative purposes and in accordance with
administrative regulations. Limited personal use of the system shall be permitted if the use:
1. Imposes no tangible cost on the District
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.
4. Any system user identified as a security risk or having violated District computer-use guidelines may be denied access to the Newcastle ISD system.

• E-Mail Access

Students may be given an e-mail account by the school utilizing a contracted monitored e-mail service Students may access their monitored e-mail service only before or after

school unless access to a message is a classroom activity assigned by the teacher. Students desiring an e-mail account will be assessed an annual fee for usage. Teachers are given an Internet e-mail account with Region 9 Service Center and have access to Microsoft Mail via our Local Area Network for local e-mail within our building.

The Technology Coordinator is authorized to monitor or examine all system activities including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the system. All users will be required to sign a user agreement annually for issuance of an e-mail account.

• Chat Rooms

No participation on any chat room accessed on the Internet is permissible for students or employees.

• Local Area Network User Accounts

Students in grades 8-12 will be allowed a folder on the network server. This folder can be used to store data produced as part of class assignments. The student logging on to the network with user identification and a password will access this folder. Only the designated student a teacher needing access to data in the student folder and the system administrator can access a student folder. It is the responsibility of the student to protect his password and not give access to any other student. Failure to meet this responsibility will be a violation of his acceptable use agreement and will mean revocation of his use of the system network.

Students in grades K-6 will be allowed to save data on the network in a folder created and assigned to the classroom teacher. The teacher will be responsible for accessing the folder for the students.

Any system user identified as a security risk or as having violated District computer use guidelines may be
denied access to the District's system.

The technology coordinator will set limits for data storage within the District system.

All users will be required to sign a user agreement annually for issuance or renewal of an account.

District Web Site

The District will maintain a District Web site for the purpose of informing employees, students, parents and members of the community of District programs, policies, and practices. Request for publication of information on the District Web site must be directed to the designated Webmaster. The technology

coordinator and the District Webmaster will establish guidelines for the development and format of Web pages controlled by the District.

No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.

No commercial advertising will be permitted on a Web site controlled by the District.

• Class and Extra Curricular Organization Web Pages

School or classes may publish and link to the District's site, Web pages that present information about the school or class activities, subject to approval from the Webmaster.

With approval of the District Webmaster, extracurricular organizations may establish Web pages linked to the District Web site; however, all materials presented on the Web page must relate specifically to organization activities and include only student-produced material. The sponsor of the organization will be responsible for compliance with District rules for maintaining the Web page. Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District." Any links from the Web page of an extracurricular organization to sites outside the District's computer system must receive approval from the District Webmaster

• Teacher Web Pages

Teachers will be responsible for compliance with District rules in maintaining their class Web pages. Any links from a school or class Web page to sites outside the District's computer system must receive approval from the District Webmaster.

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.

Acceptable Use

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Non-compliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District.

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. System user may not use another person's system account without permission from system administrator.
6. Students may not distribute personal information about themselves or other classmates. This includes, but is not limited to, personal address and telephone numbers.
7. Students should never make appointments to meet people whom they meet on-line and should report to a teacher or administrator if they receive any request for such a meeting.
8. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with District regulations.
9. System users should avoid actions that are likely to increase the risk or introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
10. System users must get permission from the system administrator to download public domain programs.
11. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation or illegal.
12. System user may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
13. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school whether or not that was the user's intention.

• Network Etiquette

System users are expected to observe the following network etiquette:
1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving a message is considered inappropriate.
4. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's account and equipment.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

• Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Vandalism to workstation equipment will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences (Student Code of Conduct.)

• Forgery Prohibited

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

Revocation

A student knowingly bringing prohibited material into the school's electronic environment or violated any
policy outlined in this document will be subject to suspension of access and revocation of privileges on the
District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment or violated any policy outlined in this document will be subject to disciplinary action in accordance with District policies.