

## **Student Acceptable Use Policy**

### **Technology Mission Statement**

Leadership Prep is committed to utilizing the maximum potential of technology to enhance student learning and increase teacher effectiveness by providing students with technology-related experiences. Recognizing the ever-changing influences of technology on all aspects of our lives, Leadership Prep is dedicated to providing an integrated technological curriculum for all students and staff members. Students will have access to the technology necessary to produce, manage, communicate and retrieve information in an efficient manner for educational use. In the attainment of both present and future goals, Leadership Prep will provide a continually evolving staff development program oriented toward the integration of technology in areas of curriculum.

### **Instructional Resource**

Leadership Prep is proud to bring network and Internet access to school employees and students. Leadership Prep believes the Internet offers many diverse and unique resources to both students and staff. Leadership Prep's goal in providing this service to staff and students is to promote educational excellence in schools by facilitating resource sharing, innovative teaching, and communication skills.

Students and staff have access to numerous research oriented and instructional resources via the Internet. On-line encyclopedias, professional journals, and databases filled with timely information on thousands of topics are just a few of the resources provided. On-campus computers have the technology necessary to support student research and to promote academic achievement.

### **Student Safety**

Leadership Prep is aware that resources which are inappropriate or not designed for use in the educational setting may be accessed on the Internet. To protect students and staff from such inappropriate material, the school's Internet access is filtered with one of the highest-rated Internet filtering systems available. However, users must recognize that it is impossible for Leadership Prep to restrict access to all controversial material and individuals must be responsible for their own actions in navigating the network.

### **Purpose**

The purpose of this policy is to ensure school-level compliance with all procedures and regulations regarding the local area network and Internet usage. All students, parents, teachers, administrators and school employees who obtain their Internet access through Leadership Prep are expected to use these services appropriately.

### **User Responsibilities**

1. The use of the Internet is a privilege. Abusive conduct will lead to the privilege being revoked. Leadership Prep is providing Internet resources for educational purposes only. Student/staff use of Internet resources must be related to an expressed educational and/or administrative goal or objective.
2. The use of Leadership Prep Internet and computer network must be in support of educational goals, research, and class assignments and be consistent with the educational objectives of Leadership Prep.
3. Users must have a valid, authorized account to access the network, and use only those computer resources that are authorized. Accounts may be used only in accordance with authorized purposes.
4. Individual accounts may be used only by the owner of the account except where specifically

authorized by school administrators. In the case of class accounts, all use must be under the supervision of the sponsoring teacher/supervisor.

5. The user is responsible for safeguarding the computer account. Users are expected to protect access to accounts by periodically changing the password and keeping it confidential. They must respect the privacy of others by not tampering with their files, passwords or accounts.

## **Policy – Terms and Conditions**

### Acceptable Use

Users are to properly use school network resources for educational and/or administrative purposes. Respectful and responsible network etiquette and behavior should be in keeping with Leadership Prep's mission statement. Students and staff are expressly prohibited from accessing obscene, profane, vulgar, or pornographic sites or materials.

Students are prohibited from sending or posting electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation or illegal. This prohibition applies to conduct off school property if it results in a substantial disruption to the educational environment. Any person taking, disseminating, transferring or sharing obscene, sexually oriented, lewd or otherwise illegal images or other content will be disciplined according to the Student Code of Conduct and may, in certain circumstances, be reported to law enforcement. Because engaging in this type of behavior can lead to bullying or harassment, students involved in "sexting" or the sharing of inappropriate images or other content may also be disciplined for violating the school's anti-harassment and bullying policies.

### Monitored Use

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated school staff to ensure appropriate use for educational or administrative purposes. Forgery or attempted forgery of electronic mail messages is prohibited. Only authorized school personnel designated by the Director of Technology Services, may 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. Forgery or attempted forgery will result in the cancellation of system privileges, as well as other appropriate consequences.

### Vandalism

Vandalism is defined as any malicious attempt to harm, disrupt or destroy data of another user of Leadership Prep's network, or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creating of computer viruses. Any of these actions may be viewed as violations of school policy, administrative regulations and, possibly, as criminal activity under applicable state and federal laws. Users must respect the privacy of other users. Users will not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user. Deliberate attempts to degrade or disrupt system performance and/or degrade, disrupt, or bypass system security are violations of school policy and administrative regulations and may constitute criminal activity under applicable state and federal laws.

Any prohibited behavior under this policy will result in the cancellation of technology privileges. Leadership Prep will in accordance with school policy, cooperate with local, state, or federal officials in any investigation concerning or relating to misuse of Leadership Prep's network.

### Network Etiquette

The user is expected to exhibit the following behavior:

1. Be polite (i.e. an all caps message implies shouting);
2. Use appropriate language;
3. Refrain from any activity that may be considered “cyber bullying,” including but not limited to threats of violence, extortion, obscene or harassing messages, harassment, stalking, child pornography, and sexual exploitation;
4. Maintain confidentiality of the user, colleagues, and students;
5. Respect copyright laws;
6. Be respectful in all aspects of network use.

### **Consequences**

Violation of school policies and procedures concerning use of the computer on the networks will result in the same disciplinary actions that would result from similar violations in other areas of school life. Any or all of the following student consequences may be enforced:

- Loss of computer privileges/Internet access, with length of time to be determined by campus administration.
- Any campus-based disciplinary consequence as deemed appropriate by the administration.
- Suspension may be considered for flagrant violations or violations that corrupt the educational value of the computers or the Internet.
- Expulsion may be considered in instances where students have used school Internet access to engage in conduct that constitutes felony criminal mischief, and/or have deliberately attempted to bypass installed security software or copy/modify another student’s work files.
- Criminal prosecution, if applicable.

## **RESPONSIBLE USE AGREEMENT**

Your child will be expected to abide by the following generally accepted rules of network etiquette.

### **NETWORK GUIDELINES**

#### **1. PERSONAL SAFETY**

- a. I will not post personal contact information about myself or other people for public view. Personal contact information includes my address or telephone number. (safety violation)
- b. I will not agree to meet with someone I have met online without my parent’s approval. (safety violation)
- c. I will promptly disclose to my teacher or other school employee any message I receive that is inappropriate or makes me feel uncomfortable. (safety violation)
- d. I will not engage in cyber-bullying including personal attacks and/or threats on/against anyone made while using district owned technology to access the Internet or local school networks. Any acts of this kind should be reported to responsible school personnel. (safety violation)
- e. I will follow the rules of netiquette and conduct myself in a responsible, ethical and polite manner. (safety violation)

#### **2. ILLEGAL ACTIVITY**

- a. I will not attempt to gain unauthorized access to my school’s file servers or to any other computer system that goes beyond my authorized access. This includes attempting to log in through another person’s files. These actions are illegal, even if only for the purposes of “browsing”. (theft)
- b. I will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal. (vandalism)
- c. I will not use my school’s file servers to engage in any other illegal activity such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, or threatening the safety of a person. (drug and safety violation)
- d. I will not read, move, rename, edit, or in any way alter the files that have been created or organized

by others. (vandalism)

e. I will not alter hardware or software set-ups on my school's computers or the file servers. (vandalism)

### 3. SECURITY

a. I am responsible for my individual account and should take all reasonable precautions to prevent others from being able to use my account. Under no conditions will I provide my password to another person. (safety violation)

b. I will immediately notify a teacher or the system administrator if I have identified a possible security problem. I will not go looking for these security problems, because this may be construed as an illegal attempt to gain access. (safety violation, theft)

c. I will avoid the inadvertent spread of computer viruses by following the district's virus protection procedures. (vandalism)

### 4. INAPPROPRIATE LANGUAGE

a. Restrictions against inappropriate language applies to public messages, private messages, and material created for assignments or to be posted on web pages. (Derogatory statements, disruption of education)

b. I will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. (derogatory statement, sexual harassment)

c. I will not engage in personal attacks, including prejudicial or discriminatory attacks. (derogatory statements, disruption of education)

d. I will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If I am told by a person to stop sending them messages, I will stop. (disrespecting others' rights, disruption of education)

e. I will not knowingly or recklessly post false or defamatory information about a person or organization. (derogatory statements, disruption of education)

### 5. RESPECT FOR PRIVACY

a. I will not re-post a message that was sent to me privately without permission of the person who sent me the message. (disrespecting other's rights)

b. I will not post private information about another person. (disrespecting other's rights)

### 6. RESPECTING RESOURCE PERMITS

a. I will use the technology at my school only for educational and career development activities. (disruption of education)

b. I will not download large files unless absolutely necessary. (disruption of education)

c. I will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people. (disruption of education)

### 7. PLAGIARISM AND COPYRIGHT INFRINGEMENT

a. I will not plagiarize works that I find on the Internet or on the computers at my school. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own. (theft)

b. I will respect the rights of copyright owners. Copyright infringement occurs when I inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, I will follow the expressed requirements. If I am unsure whether or not I can use a work, I will request permission from the copyright owner. If I am confused by copyright law, I will ask a teacher to answer my questions. (theft)

c. I will follow copyright laws and should only download/import music or other files to a district owned technology that he/she is authorized or legally permitted to reproduce, or for which he/she has the copyright.

## 8. INAPPROPRIATE ACCESS TO MATERIAL

In accordance with the Children's Internet Protection Act (CIPA) the district has an Internet appliance that blocks access to pictures that are obscene, child pornography or harmful to minors. Individuals will abide by the following policies:

- a. I will not use my school's file servers to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination toward other people. (disruption of education, safety violation)
- b. If I mistakenly access inappropriate information, I will immediately tell my teacher or an administrator. This will protect me against a claim that I have intentionally violated this policy. (failing to comply with directives)
- c. My parents will instruct me if there is additional material that they think would be inappropriate for me to access. The district fully expects that I will follow my parent's instructions in this matter. (respect for others violation)

## STUDENT'S RIGHTS

### 1. SEARCH AND SEIZURE

- a. I should expect only limited privacy in the contents of my personal files on my school's server. The situation is similar to the rights I have in the privacy of a locker.
- b. Routine maintenance and monitoring of each school's file server may lead to discovery that I have violated this network guideline, the district's Student Code of Conduct, or the law.
- c. An individual search will be conducted if there is reasonable suspicion that I have violated the network guidelines, the district's code of Conduct, or the law. The investigation will be reasonable and related to the suspected violation.
- d. My parents have the right at any time to see the contents of my files.

### 2. DUE PROCESS

- a. The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through a school's or the district's file servers.
- b. In the event there is a claim that I have violated the network guidelines or the district's Student Code of Conduct in my use of the school's or district's file servers, I will be provided with notice and opportunity to be heard in the manner set forth in the district's Student Code of Conduct.
- c. If the violation also involves a violation of other provisions of the district's Student Code of Conduct, it will be handled in a manner described in that code of conduct. Additional restrictions may be placed on the use of my account.

### 3. LIMITATION OF LIABILITY

The district makes no guarantee that the functions or the services provided by or through the district's system will be error-free or without defect. The district will not be responsible for any damage I may suffer including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stores on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

### 4. CARE AND USE

I will keep my laptop secure and damage free. Each laptop is issued with a protective bag; use of the laptop bag is required at all times. Follow these general guidelines:

- Do not loan the laptop or charger and cords.
- Do not forcefully close the laptop when shutting it down or putting it to sleep.
- Do not leave the laptop in a location exposed to extreme temperatures or water.
- Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.

- Do not stack objects on top of the laptop.
- Do not leave the laptop in a location where it could be damaged: on the floor, near table or desk edges, in the presence of small children or pets, in luggage where it could be crushed.

## 5. PERSONAL RESPONSIBILITY

I understand that I am responsible for the district's technological hardware that I use. My use of the technology available to me at school can be a mirror that will show what kind of person I am. This may result in damage not covered by warranties, in which case I will be liable for repair costs.

I will not connect any personal technologies such as laptops and workstations, wireless access points and routers, printers, etc. to district owned and maintained local, wide or metro area networks. Connection of personal devices such as iPods, smartphones, tablets, PDAS and printers are permitted but not supported by LPS technical staff or LPS administration in case of theft or loss. Home Internet use is the responsibility of the student both in cost and configuration.

I will back up data and other important files regularly. LPS will at times maintain the laptops by imaging. All files not backed up to server, cloud storage or other storage media will be deleted during these processes. Students are ultimately responsible for backing up all personal files on their own storage media.

## STUDENT PLEDGE

1. I will adhere to personal safety guidelines. I will keep personal information private, report any inappropriate conduct or cyber-bullying and follow proper netiquette.
2. I will only engage in legal activity. I will only access or alter files that have been made available to me. I will respect the computer system, network, hardware and software.
3. I will maintain my account security. I will notify a responsible district employee of a security problem.
4. I will only use appropriate language. I will be courteous to other users, my campus and school district. I will report any personal attacks, disrespectful language, harassment, or defamation to a responsible district employee.
5. I will respect message privacy and personal privacy and only repost messages and information that I have received consent to post.
6. I will only use the technology issued by my campus and district for educational, college and career development purposes. I will only download files necessary for these purposes and report any instance of spamming to a responsible district employee.
7. I will adhere to copyright laws. I will respect the rights of copyright owners and only download authorized and legal copies of information, including music.
8. I will access only appropriate materials and report any profane or obscene information or images to a responsible district employee.
9. I realize my district issued laptop is subject to search and seizure. I will cooperate with district officials in any case of investigation.
10. I will take care of my laptop and avoid any act that could void the warranty, realizing I am responsible for any misuse. I will use only my district issued laptop for classroom activities and backup my data periodically.