

La Grange Highland School District 106
DISTRICT OWNED INFORMATION ASSETS ACCEPTABLE USE RULES & REGULATIONS

The goal of the School Board is to promote the appropriate use of District owned information assets for the purpose of increasing educational opportunities and academic performance, facilitating communication between parents, colleagues, and students, and conducting research to further the curricular and professional goals of the District.

All use of District owned information assets shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These rules and regulations do not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.** The District Acceptable Use Rules and Regulations applies to all users of La Grange Highlands School District 106 District owned information assets.

District owned information assets, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication.

The School district is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose.

Privileges

Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials. Inappropriate use will result in a cancellation of privileges, disciplinary action, including but not limited to termination of employment, and/or appropriate legal action.

Internet Safety

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,

4. Restrict unauthorized access, including “hacking” and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the District’s *Authorization for Electronic Network Access* as a condition for using the District’s electronic network. Each student and his or her parent(s)/ guardian(s) must sign the *Authorization* before being granted use.

All users of the District’s computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

The failure of any student or staff member to follow the terms of the *Authorization for Electronic Network Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Monitoring

The Superintendent or his/her designee shall monitor the activities of users of District 106 information assets visually, via tracking software, logs, or remote access at any time. Other monitoring may occur as described in the *District 106 Information Security Policy* and/or the District 106 Information Technology Procedures Manual.

Unacceptable Use

Any use which disrupts the proper and orderly operation and discipline of schools in the District; threatens the integrity or efficient operation of the District computer network; violates the rights of others; is socially inappropriate or inappropriate for a student’s age or maturity level; is primarily intended as an immediate solicitation of funds; is illegal or for illegal purposes of any kind; or constitutes gross disobedience or misconduct is an unacceptable use. Use of the District computer network for any unacceptable use will result in a cancellation of privileges, disciplinary action, including but not limited to termination of employment, and/or appropriate legal action. Some examples of unacceptable uses are, but not limited to, the following:

- A. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;
- B. Unauthorized downloading of software, regardless of whether it is copyrighted or clear of viruses;
- C. Using the network for private financial or commercial gain, including gambling;
- D. Not following District procedures for using resources, such as file space, printing supplies, etc.;
- E. Using resources such as file space, printing supplies, etc. for non-school related projects without prior authorization from the Director of Technology, in consultation with the appropriate building principal;
- F. Gaining unauthorized access to resources or entities;
- G. Invading the privacy of individuals;
- H. Posting anonymous messages;
- I. Using the network for commercial or private advertising;

- J. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
- K. Using the network while access privileges are suspended or revoked;
- L. Using or accessing another user's computer network account or password, with or without consent from that user;

Network Etiquette

When using email, users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- A. Be polite. Do not become abusive in user messages to others.
- B. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- C. Do not reveal personal information such as addresses or telephone numbers of students or colleagues.
- D. Recognize that electronic mail (email) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
- E. Do not use the network in any way that would disrupt its use by other users.
- F. All information sent onto the Internet should be treated as if it could be read by anyone.

No Warranties

The District makes no warranties of any kind, whether express or implied for the service of providing computer network access to its users, and bears no responsibility for the accuracy or quality of information or services obtained from the computer network or any loss of data suffered in connection with use of the computer network. The District will not be responsible for any damages any user suffers, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by users' errors, omissions, or negligence. Use of any information obtained from the computer network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the computer network.

The District has acted in good faith and in a reasonable manner in selecting and implementing filtering software, blocking software, and other technology protection measures to prevent access to material which is obscene, pornographic, or, with respect to use of computers by minors, harmful to minors. Nevertheless, by using the District's computer network, users acknowledge that such technology measures do not prevent access to all prohibited material, and may prevent access to non-prohibited material. The District assumes no responsibility for access gained or denied by the technology protection measures that have been implemented.

Telephone Charges

The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs, relating to, or arising out of, an individual user's use of the computer network.

Indemnification

The user agrees to indemnify the District for any losses, costs, damages, charges or fees, including, but not limited to, telephone charges, long distance charges, per-minute surcharges, equipment or

line costs, or attorney fees, incurred by the District and relating, or arising out of the user's use of the District's computer network or any violation by the user of the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of computer network access promulgated by the Superintendent, Building Principals, or the Director of Technology.

Security

Network security is a high priority. Users must keep their account name and password absolutely confidential. Attempts to log-on a District owned information asset as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism

Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Cooperation with Investigations

The District reserves the right to participate and cooperate fully in any investigation requested or undertaken by either law enforcement authorities or a party alleging to have been harmed by the use of the District computer network. Evidence of illegal activity may be reported or turned over to appropriate authorities.

Enforcement

The failure of any user to abide by the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of computer network access promulgated by the Superintendent, Building Principals, or the Director of Technology will result in the suspension or revocation of the user's computer network privileges, disciplinary action, including but not limited to termination of employment, and/or appropriate legal action. Computer network privileges may be suspended or revoked by the Superintendent or Building Principal with the recommendation of the Director of Technology. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies.

Policy Modifications

The Board of Education may modify the terms and conditions of use and/or the provisions of this Policy and its implementing Rules and Regulations at any time. The Superintendent, Building Principals, or Director of Technology may also promulgate additional rules, regulations, or other terms or conditions of computer network access as may be necessary to ensure the safe, proper, and efficient operation of the computer network and the individual District schools. Notice of any such modifications or additional rules, regulations, or other terms of conditions of access shall be promptly communicated to all authorized users, including by posting such modifications on the computer network or in a conspicuous place at access locations. Use of the computer network constitutes acceptance of the terms of the Policy, these Rules and Regulations, and any additional rules, regulations, or other terms or conditions of computer network access which may have been promulgated by the Superintendent, Building Principals, or their designees.

Publication of Student Work and/or Pictures

In furtherance of the School Board's stated goal, La Grange Highlands School District 106 website has been developed. Through this site, increased communication between students, parents, teachers and other entities will be achieved. From time to time the school may wish to publish examples of student projects, photographs of students, and other work on an Internet accessible World Wide Web server. Student faces will not be posted on the World Wide Web site of District 106 without prior written authorization from a parent or guardian. Student work posted to the District 106

World Wide Web server will be identified by first name only and will not be accompanied by an individually identifiable image of the student.

Reporting Procedures for Suspected AUP Violations

District 106 mandates that anyone who believes that there is a violation of this AUP direct the information to the Director of Technology or Superintendent in writing or via email.

If available, please provide the following information:

1. The exact nature of the alleged violation
2. Explain how you came to learn of this violation
3. The date and time of the alleged violation
4. Evidence of the alleged violation

If you believe the violation is email related, please DO NOT delete, move, or change the message in any way. Email with full header information provides many of the clues necessary to investigate possible email abuse violations.

School District 106 will cooperate with all law enforcement agencies (local, state, and federal) in their investigatory pursuits related to data transmission originating from District 106 networks and servers. There is no guarantee that email generated on or received by District 106 network/services will remain private.

Parent/Student Authorization for Electronic Network Access

Dear Parents/Guardians:

Our School district has the ability to enhance your child's education through the use of electronic networks, including the Internet. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication. Students and their parents/guardians need only sign this *Authorization for Electronic Network Access* once while the student is enrolled in the School District.

The District *filters* access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate in the school setting. If a filter has been disabled or malfunctions it is impossible to control all material and a user may discover inappropriate material. Ultimately, parents/guardians are responsible for setting and conveying the standards that their child or ward should follow, and the School District respects each family's right to decide whether or not to authorize Internet access.

With this educational opportunity also comes responsibility. The use of inappropriate material or language, or violation of copyright laws, may result in the loss of the privilege to use this resource. Remember that you are legally responsible for your child's actions. If you agree to allow your child to have an Internet account, sign the *Authorization* form below and return it to your school.

Authorization for Electronic Network Access Form

Students must have a parent/guardian read and agree to the following before being granted unsupervised access:

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. **The failure of any user to follow the terms of the *Acceptable Use of Electronic Networks* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

I have read this *Authorization* form. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the *Acceptable Use of Electronic Networks* with my child. I hereby request that my child be allowed access to the District's electronic network, including the Internet.

Parent/Guardian Name (please print)

Parent/Guardian Signature

Date

Students must also read and agree to the following before being granted unsupervised access:

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my email and downloaded material, without prior notice to me. I further understand that should I commit any violations, my access privileges may be revoked, and school disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic network, including the Internet.

Student Name (please print)

Student Signature

Date

Permission for Publication:

My child listed above, may be photographed or videotaped for publication.

Yes No

Parent/Guardian Name (please print)

Parent/Guardian Signature

Date

Staff and Non-Student Authorization for Electronic Network Access

All use of the Network shall be consistent with the District’s goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or proscribed behavior by users, however, some specific examples are provided. **The failure of any user to follow the terms of Administrative Procedure 6:235-AP1, *Acceptable Use of Electronic Networks*, will result in the loss of privileges, disciplinary action, and/or legal action.** The signature at the end of this document is legally binding and indicates that the individual has read the terms and conditions carefully and understand their significance.

Staff members need only sign this *Authorization for Electronic Network Access* once while employed by the School District.

I understand and will abide by the *Acceptable Use of Electronic Networks*. I understand that the District and/or its agents may access and monitor my use of the District’s electronic network, including the Internet, my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and disciplinary action and/or legal action may be taken. In consideration for using the District’s electronic network connection and having access to public networks, I hereby release the School District and its School Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District’s electronic network, including the Internet.

User Name (*please print*)

User Signature

Date