

Lynwood Unified School District

Acceptable Use Policy (AUP) for District Computer Systems

Information for Parents and Students

Objectives

The District's Acceptable Use Policy ("AUP") has been developed to ensure security and reliability of our systems and network and the networks and systems of others, prevent unauthorized access and other unlawful activities by users online, and to prevent unauthorized disclosure of or access to sensitive information. The District will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network, as required by the Children's Internet Protection Act ("CIPA").

The District reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network, and/or Internet access or files, including email.

As used in this policy, "user" includes anyone using the computers, Internet, email, chat rooms, and other forms of direct electronic communications or equipment provided by the District (the "network."). **Only current students or employees are authorized to use the network.**

Acknowledgement of Policy

Schools must verify each year students using the computer network and Internet access for that school year have a signed page acknowledging this policy. Students who are under 18 must have their parents or guardians sign this page and schools must keep it on file. Once signed that permission/acknowledgement page remains in effect until revoked by the parent, or the student loses the privilege of using the District's network due to violation of this policy, or is no longer a District student. Employees and other users are required to follow this policy. Even without signature, all users must follow this policy and report any misuse of the network or Internet to a teacher, supervisor or other appropriate District personnel. Access is provided primarily for education and District business. Staff may use the Internet, for incidental personal use during duty-free time. **By using the network, users have agreed to this policy.** If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor or other appropriate District personnel.

Unacceptable Uses of the Computer Network or Internet

- **Transmitting on or through the network any material that is, in the District's sole discretion, unlawful, threatening, abusive, libelous, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state, national or international law, statute or regulation.**
- **Accessing or transmitting pornography of any kind, obscene depictions, harmful or offensive materials, materials that encourage others to violate the law, confidential information, or copyrighted materials;**
- **Selling or purchasing illegal items or substances;**
- **Using anonymous email websites, spreading SPAM (unsolicited email), "chain letters," or viruses;**
- **Causing harm to others or damage to their property, such as:**
 1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others;
 2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
 3. Disrupting services, destroying data, destroying or damaging equipment, or disrupting the operation of the network in any way, including the intentional distribution or posting of any virus, worm, Trojan horse, or computer code intended to cause harm;
- **Users may not attempt to circumvent user authentication or security of or jeopardize access to any host, network, or account. This includes, but is not limited to:**
 1. Accessing data the user is not expressly authorized to access;
 2. Probing the security of the District's network and the networks of others, password sniffing, IP spoofing;
 3. Using another's account password(s) or identifier(s);
 4. Interfering with other users' ability to access their account(s); or
 5. Disclosing anyone's password to others or allowing them to use another's account(s).
- **Using the network or Internet for Commercial purposes:**

1. Using the Internet for personal advertising, promotion, or financial gain; or;
2. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

Student Internet Safety

1. Students under the age of eighteen should only access District accounts outside of school if a parent or legal guardian supervises their usage at all times. The student’s parent or guardian is responsible for monitoring the minor’s use;
2. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students may not reveal their name, home address, telephone number, or display photographs of themselves or others;
3. Students shall not meet in person anyone they have met only on the Internet; and
4. Students must abide by all laws, this Acceptable Use Policy, and all District security policies.

Confidentiality

Users with access to confidential data are to utilize all appropriate precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur.

Penalties for Improper Use

The use of the District network is a privilege, not a right, and misuse will result in the restriction or cancellation of the use. The principal, teacher, site administrator, supervisor, or systems administrator may limit, suspend, or revoke access to the network at any time. Misuse may also lead to disciplinary (including suspension or termination) and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations that result or have alleged to have resulted from the use of or inability to use the network; or that results from mistakes, omissions, interruptions, deletion of files, loss of data, errors, defects, delays in operations, or transmission or any failure of performance, communications failure, theft, destruction or unauthorized access to the District’s records, programs, or services. The District further denies any responsibility for the accuracy or quality of information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

I have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Lynwood Unified School District.

Date: _____	School: _____
Student Name: _____	Student Signature: _____
Parent/Legal _____	Parent/Legal _____
Guardian Name: _____	Guardian Signature: _____

Please return this form to the school where it will be kept on file. It is required for all students that will be using a computer network and/or Internet access.