

# COMMUNITY UNIT DISTRICT #205 WARREN JR/SR HIGH SCHOOL INTERNET ACCEPTABLE USE POLICY

## INTRODUCTION

Internet access is available to students, teachers, and administrators of Community Unit District #205. We are happy to offer these services and believe it offers vast, diverse, and unique resources to both students and teachers. Our goal is to promote educational excellence for students of the district by enhancing our resources and communication.

## APPLICATION FOR INTERNET ACCESS

Internet access is a privilege that must be earned. Anyone expecting to access the Internet in our school must do the following:

1. Read, sign, and turn in the Computer Use form (one time but initialed each year).
2. Read, sign, and turn in the Internet Acceptable Use Policy form (yearly).
3. Go through the process to earn an Internet Driver's License (one time).

The failure of any user to follow the terms of this Acceptable Use Policy (AUP) will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The consequences for failure to follow this Acceptable Use Policy include, but are not limited to, the following:

First violation - license is punched and loss of privileges for 1 week

Second violation - license is punched and loss of privileges for 1 month.

Third violation - license is punched, loss of privileges for 1 calendar year and student must go through process to obtain a second license

First violation with second license - loss of privileges forever

Any violation of this AUP that also constitutes a violation of any federal, state, or local law will result in loss of privileges forever. The signature at the end of this document is binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

## TERMS AND CONDITIONS

1. Acceptable Use – Access to the District's electronic network must be for the purpose of education or research and be consistent with the educational objectives of the District.
2. Privileges – The use of the District's computer network and Internet connection is a privilege, not a right, and inappropriate use will result in a loss of those privileges, disciplinary action, and/or appropriate legal action as provided above. Computer network privileges may be suspended or revoked and Internet driver's licenses may be punched by the Superintendent, Building Principal, or Technology Coordinator. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies.
3. Unacceptable Use – You are responsible for your actions and activities involving the network. 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 the loss of computer network privileges, disciplinary action, and/or appropriate legal action. Some, but not all, examples of unacceptable uses include, **but are not limited to**, the following:
  - Using the network for non-educational games as this places a heavy load on scarce resources - a list of permissible games will be posted in the lab and library; if it is not on the list, it is not acceptable
  - Unauthorized downloading of material, regardless of whether it is copyrighted or devious
  - Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any federal, state, or local law or community standards
  - Printing copyrighted material for other than personal research

- Using the network for private financial or commercial gain
- Wastefully using resources such as file space
- Gaining unauthorized access to resources or entities
- Invading the privacy of individuals
- Using another user's account or password
- Posting material authored or created by another without his/her consent
- Posting anonymous messages
- Commercial or private use of the network
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, harassing, or illegal material
- Using the network while access privileges are suspended or revoked.
- Using the Internet in any way which is not stated as an intended use on the student's Internet pass; and
- Attempting to commit any action which would constitute an unacceptable use if accomplished successfully.

Trying to circumvent the filter – this will lead to an immediate suspension, loss of computer network privileges, appropriate legal action, and board notification. The student will also be responsible for any financial costs incurred by the District due to the above actions.

4. Network Etiquette – You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Be polite. Do not become abusive in your messages to others.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- Do not reveal personal information about you or anyone else.
- Do not use the network in any way that would disrupt its use by other users.

5. Internet Safety – The District's primary concern in maintaining Internet access is that student safety and security not be compromised at any time. Some of the most effective safety measures can only be implemented by students themselves. The District encourages parents and guardians to discuss the following safety concerns with their students:

- Students should immediately inform their parents, guardians, or a member of District staff if they come across any information on the Internet or in an e-mail that makes them feel uncomfortable. Students should not respond to any e-mail or other message which makes them feel uncomfortable.
- Students should never agree to meet someone in person whom they have "met" online without parental knowledge, permission, and supervision.
- Students should never agree to send or accept any item to or from a person whom they have "met" online without parental knowledge, permission, and supervision.

6. Technology Protection Measures – Consistent with the District's legitimate educational and pedagogical concerns, the District has implemented technology protection measures designed to filter or block access to objectionable or inappropriate material through the District's Internet connection. These measures are implemented in the best manner practicable to prevent access to any material, including visual depictions, which is obscene; which constitutes pornography, including child pornography; or which, with respect to use of computers by minors, would be harmful to minors. The Superintendent, Building Principals, or Technology Coordinator may disable the technology protection measure to allow non-student adults to access material needed for bona fide research or other lawful purpose.

7. Monitoring of Student Internet Use – The District shall monitor the use of the Internet by students and any other minor users in order to ensure compliance with the AUP and other rules, regulations, or other terms or conditions of computer network and Internet access promulgated by the Superintendent, Building Principals, or Technology Coordinator and other disciplinary policies and regulations necessary to further the educational, safety, and pedagogical concerns of the District.

8. No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its service. 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 and Internet connection, 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.

9. Indemnification – The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any use of the District's computer network or Internet connection or any breach of this Authorization.
10. Security – Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. Attempts to log-on to the Internet as a system administrator will result in loss of privileges forever and other appropriate disciplinary and/or legal action.
11. Vandalism – Vandalism will result in loss of privileges forever and other appropriate disciplinary and/or legal action. Vandalism is defined as any intentional 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.
12. 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.
13. Use of Electronic Mail – Mail accounts **will not** be accessed at school. Students are not allowed to access personal email accounts at school such as Hotmail, Yahoo mail, Excite mail, etc. Students accessing these accounts will receive a punch on their license.
14. Copyright Web Publishing Rules – Copyright law and District policy prohibits the republishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission.
  - Students may not publish web pages from school.
  - Student work may only be published by a staff member if there is written permission from both the parent/guardian and student.
15. Use of material on the Internet for reports, term papers, etc.
  - The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
  - Do not plagiarize material.

## **PROCEDURE**

1. Secure a pass from a member of the district staff stating the purpose for using the Internet.
2. Inform the supervisor of your intent to use the Internet and show them the pass informing them of your purpose.
3. Display your Internet Driver's License on the keyboard over NumLock, CapsLock, & ScrollLock lights.
4. Log onto the network and go into Internet Explorer.
5. Keep in mind your activity can be tracked and will be checked. Keep focused on your goal. Failure to do what the pass indicates is a violation and will result in the appropriate consequence.
6. When finished, log off of the system.