DISTRICT COMPUTER SYSTEM USE AND INTERNET SAFETY POLICY

Introduction

The Board of Education of Unity Point Community Consolidated School District No. 140 hereby determines that it is in the best interests of the District, its personnel and its students, and members of the community to promote use of and familiarity with the District Computer System and with the services which are available through that System to support learning and enhance instruction, and to improve communications between the school and community.

Knowledgeable and appropriate use of the District Computer System can facilitate access to information resources available on-line, create innovative learning environments, and provide for worldwide communication. For purposes of this policy, implementing rules, and acceptable use guidelines, the term "District Computer System" or "System" shall include all computer hardware and software owned or operated by the District, District electronic mail, District web sites, and District on-line services and bulletin board systems. "Use" of the District Computer System shall include use of or obtaining access to the System from any computer terminal whether or not owned or operated by the District.

The District Computer System was established to comprise part of the school curriculum, and is intended by this Board to function in support of that curriculum and of students' mastery of the curriculum through improved communication between the school and students' parents or guardians. The District Computer System does not constitute a public forum. The District reserves and retains the right to regulate the content of and links to the District Computer System. The District also has the right to and does monitor use of its Computer System. Except as provided by federal and state statutes protecting the confidentiality of students' education records, no user of the District Computer System has an expectation of privacy in connection with such use.

Access to Inappropriate Material or Network Usage

The Board of Education recognizes that although the Internet and on-line services afford access to legitimate sources of information for academic and educational purposes, they also enable access to materials which may be illegal, obscene or indecent. The use of elements of the District Computer System including the Internet shall be consistent with the District's educational mission and the curriculum adopted by the Board.

With respect to any of its computers with Internet access, the District will use technology protection measures (or "Internet filters") to (A) protect minors against access through such computers to visual depictions which are obscene, constitute child pornography, or are otherwise harmful to minors, and (B) protect all users against access through such computers to visual depictions that are obscene or constitute child pornography.

Supervision and Monitoring

It shall be the responsibility of all members of the staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of Technology Director or designated representatives for bona fide research or other lawful purpose.

Guidelines For Acceptable Use Of District Computer System

The Board of Education further recognizes that the effective operation of the District Computer System depends upon the existence and enforcement of guidelines for the efficient, ethical and legal use of its resources. The Administration is authorized to and shall adopt and enforce guidelines which limit the use of the System to educational purposes, and describe acceptable and ethical use of the System.

The guidelines shall, among other points, address compliance with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)] to include:
:

- Access by minors to inappropriate matter on the Internet and World Wide Web;
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication;
- Unauthorized access, including "hacking" and other unlawful activities by minors and other users online;
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
- Measures designed to restrict minors' access to materials harmful to minors.

Such guidelines shall be distributed to District employees and students [and other members of the District 140 community] who are afforded access to the System.

Violation of the acceptable use guidelines shall be subject to consequences including but not limited to discipline, loss of System use privileges, and referral to law enforcement authorities or other legal action in appropriate cases.

The Board of Education of Unity Point Community Consolidated School District No. 140 adopted this Internet Safety Policy at a public meeting, following normal public notice, on April 11, 2007.

GUIDELINES FOR ACCEPTABLE USE OF DISTRICT COMPUTER SYSTEM BY STUDENTS

A. Acceptable Use.

All users of the District Computer System ("System") must comply with the District's Acceptable Use Guidelines, as amended from time to time.

The "System" shall include all computer hardware and software owned or operated by the District, the District electronic mail, the District web site, and the District on-line services and bulletin board systems. "Use" of the System shall include use of or obtaining access to the System from any computer terminal whether owned or operated by the District.

Students have no expectation of privacy in their use of the System. The District has the right to access, review, copy, delete, or disclose, as allowed by law, any message sent, received, or stored on the District's electronic mail system. The District has the right to determine access or use of the System by students and does monitor use, including students' access of the Internet, as part of System maintenance and to determine whether the use is consistent with federal and state laws and District policies and guidelines.

To the extent practical, steps shall be taken to promote the safety and security of users of the System when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Student access to aforementioned systems is limited.

B. Privileges.

Access to the System is provided as a privilege by the District and may be revoked at any time. Inappropriate use may result in discipline, including loss of System use privileges.

The System, including all information and documentation contained therein is the property of the District except as otherwise provided by law.

C. Prohibited Use.

The uses of the System listed below are prohibited and may result in discipline or other consequences as provided in section H of these Guidelines and the District's Student Discipline Code and rules. The System shall **not** be used to:

1. Engage in activities which are not related to District educational purposes or which are contrary to the instructions from supervising District employees as to the System's use.

2. Access, retrieve, or view obscene, profane or indecent materials. "Indecent materials" are those materials which, in context, depict or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.

3. Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulation or District policy or rules. This includes, but is not limited to, plagiarism; improper use of copyrighted material; improper use of the System to commit fraud or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any student, District employee, or System user.

4. Disable or otherwise modify any technology protection measures. Such action shall be the responsibility of the Technology Director or designated representatives for "bona fide research or other lawful purpose".

5. Transfer any software to or from the System without authorization from the System Administrator.

6. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.

7. Harass, threaten, intimidate, or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation.

8. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.

9. Disrupt or interfere with the System.

10. Gain unauthorized access to or vandalize the data or files of another user.

11. Gain unauthorized access to or vandalize the System or the computer system of any other individual or organization.

12. Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password or that of another user.

13. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.

14. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.

15. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.

16. Send mass electronic mail to multiple users without prior authorization by the appropriate District Administrator.

17. Conceal or misrepresent the user's identity while using the System.

18. Post material on the District's web site without the authorization of the appropriate District administrator.

D. Web sites.

Unless otherwise allowed by law, District web sites shall not display information about or photographs or works of students without written parental permission.

Any web site created by a student using the System must be part of a District-sponsored activity, or otherwise be authorized by the appropriate District administrator. All content, including links, of any web site created by a student using the System must receive prior approval by the classroom teacher or an appropriate District administrator. All contents of a web site created by a student using the System must conform with these Acceptable Use Guidelines.

The District may discipline a student whose personal web site causes, or can reasonably be expected to cause, a substantial disruption of the school environment without regard to whether the web site was created using the System.

E. Disclaimer.

The District makes no warranties of any kind whether express or implied for the System. The District is not responsible for any damages incurred, including the loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. Use of any information obtained via the System is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained through

the System. The District is not responsible for any user's intentional or unintentional access of material on the Internet which may be obscene, indecent, or of an inappropriate nature.

F. Security and User Reporting Duties.

Security in the System is a high priority and must be a priority for all users. Students are prohibited from sharing their login IDs or passwords with any other individual. Any attempt to log in as another user will result in discipline.

A user who becomes aware of any security risk or misuse of the System must immediately notify a teacher, administrator or other staff member.

G. Vandalism.

Vandalism or attempted vandalism to the System is prohibited and will result in discipline as set forth in section H of these Guidelines, and in potential legal action. Vandalism includes, but is not limited to, downloading, uploading, or creating computer viruses.

H. Consequences for Violations.

A student who engages in any of the prohibited acts listed above shall be subject to discipline, which may include: (1) suspension or revocation of System privileges, (2) other discipline including suspension or expulsion from school, and (3) referral to law enforcement authorities or other legal action in appropriate cases.

Misuse of the System by a student may be considered gross misconduct as that term is defined by the District Student Discipline Policy and rules, and a student may be subject to discipline pursuant to the Student Discipline Policy and rules. A student who believes that his/her System use privileges have been wrongfully limited may request a meeting with the building principal to review the limitation. The decision of the building principal shall be final.

GUIDELINES FOR ACCEPTABLE USE OF DISTRICT COMPUTER SYSTEM BY EMPLOYEES

A. Acceptable Use

All users of the District Computer System ("System") must comply with the District's Acceptable Use Guidelines, as amended from time to time.

The System shall include all computer hardware and software owned or operated by the District, the District electronic mail, the District web site, and the District on-line services and bulletin board systems. "Use" of the System shall include use of or obtaining access to the System from any computer terminal whether owned or operated by the District.

Employees shall monitor Student on-line activity for appropriate use. It shall be the responsibility of all staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Employees have no expectation of privacy in their use of the System. The District has the right to access, review, copy, delete, or disclose, as allowed by law, any message sent, received, or stored on the District's electronic mail system. The District has the right to determine access or use of the System by employees and does monitor use, including employees' access to the Internet, as part of System maintenance to determine whether the use is consistent with federal and state laws and District policies and guidelines.

To the extent practical, steps shall be taken to promote the safety and security of users of the System when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Employee access to aforementioned systems is limited.

Employees should be aware that their personal computer files or System use may be subject to public disclosure under the Illinois Freedom of Information Act.

Access to the System is provided to employees primarily for work-related purposes. Incidental personal use should be minimized.

B. Privileges

The System, including all information and documentation contained therein, is the property of the District, except as otherwise provided by law.

It is the responsibility of the Faculty member to whom the System is assigned, to keep System equipment clean and away from smoke, dust, magnets, food, liquid, and any other foreign material known to be harmful to the hardware or functionality of the system and to report malfunctions of hardware or software to the Technology Office. To the extent that said action causes damage to the System, repair of assigned equipment will be at the expense of the employee with replacement not assured.

The System must be made available for inventorying, inspection, updating, and or maintenance by the District Technology or Administrative Personnel at any time.

No part of the System may be moved from room to room, removed from the District, or loaned to another District Employee without Authorization from the building Administrators and the Technology Office.

C. Prohibited Use

Uses of the System listed below are prohibited and may result in discipline or other consequences provided in Section H of these Guidelines. The System shall **not** be used to:

1. Engage in activities which are inconsistent with the District's educational mission or which interferes with an employee's performance of work responsibilities.

2. Access, retrieve, or view obscene, profane or indecent materials. "Indecent materials" are those materials which, in context, depict or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.

3. Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulation or District policy or rules. This includes, but is not limited to: plagiarism; improper use of copyrighted material; improper use of the System to commit fraud, or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any student, district employee, or user.

4. Disable or otherwise modify any technology protection measures. Such action shall be the responsibility of the Technology Director or designated representatives for "bona fide research or other lawful purpose".

5. Transfer any software to or from the System without authorization from the System Administrator.

6. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.

7. Harass, threaten, intimidate, or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation.

8. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.

9. Disrupt or interfere with the System.

10. Gain unauthorized access to or vandalize the data or files of another user.

11. Gain unauthorized access to or vandalize the System, or the computer system of any other individual or organization.

12. Forge or improperly alter electronic mail messages, use an account owned by another user without authorization, or disclose the user's individual password or that of another user.

13. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.

14. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.

15. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.

16. Send mass electronic mail to multiple users without prior authorization by the appropriate District administrator.

17. Conceal or misrepresent the user's identity while using the System.

18. Post material on the District's web site without the authorization of the appropriate District administrator.

D. Web Sites

Unless otherwise allowed by law, the District web sites shall not display photographs or work of students without written parental permission.

Any web site created by an employee using the System must be part of a District-sponsored activity, or otherwise be authorized by the appropriate District administrator. All content, including links, of any web site created by an employee using the System must receive prior approval by the appropriate District administrator. All contents of a web site created by an employee using the System must conform with these Acceptable Use Guidelines. Employees may not place any personal or editorial material on the District web site or any web site created by an employee using the System.

E. Disclaimer

The District makes no warranties of any kind whether express or implied for the System. The District is not responsible for any damages incurred, including the loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. Use of any information obtained via the System is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained through the System. The District is not responsible for any user's intentional or unintentional access of material on the Internet which may be obscene, indecent, or of an inappropriate nature.

F. Security and User Reporting Duties

Security in the System is a high priority and must be a priority for all users.

Users are prohibited from sharing their login IDs or passwords with any other individual. Any attempt to log in as another user will result in consequences as set forth in Section H of these Guidelines.

A user who becomes aware of any security risk or misuse of the System must immediately notify the appropriate District administrator.

G. Vandalism

Vandalism or attempted vandalism to the System is prohibited and will result in consequences as set forth in Section H of these Guidelines. Vandalism includes, but is not limited to, the downloading, uploading, or creating computer viruses.

H. Consequences For Violations

Any user of the System who knowingly and purposefully engages in any of the prohibited acts as listed above shall be subject to disciplinary consequences.

GUIDELINES FOR ACCEPTABLE USE OF DISTRICT COMPUTER SYSTEM BY COMMUNITY MEMBERS

A. Acceptable Use

All users of the District Computer System ("System") must comply with the District's Acceptable Use Guidelines, as amended from time to time.

The "System" shall include all computer hardware and software owned or operated by the District, the District electronic mail, the District web site and the District on-line services and bulletin board systems. "Use" of the System shall include use of or obtaining access to the System from any computer terminal whether or not owned or operated by the District.

Users shall monitor Student on-line activity for appropriate use. It shall be the responsibility of all users to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Users have no expectation of privacy in their use of the System. The District has the right to access, review, copy, delete or disclose, as allowed by law, any message sent, received or stored on the District's electronic mail system. The District has the right to determine access or Use of the System and does monitor use, including users' access to the Internet, as part of System maintenance to determine whether the use is consistent with federal and state laws and District policies and guidelines.

To the extent practical, steps shall be taken to promote the safety and security of users of the System when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. User access to aforementioned systems is limited.

B. Privileges

Access to the System is provided as a privilege by the District and may be revoked at any time. Inappropriate use may result in consequences including the loss of System use privileges. [The District will not provide community members with electronic mail accounts or access to chat groups, chat rooms and chat lines.]

The System, including all information and documentation contained therein, is the property of the District, except as otherwise provided by law.

C. Prohibited Use

Uses of the System listed below are prohibited and may result in consequences as provided in Section G of these Guidelines. The System shall **not** be used to:

1. Engage in activities which are inconsistent with the District's educational mission or which are contrary to the instructions from supervising District employees regarding the System's use.

2. Access, retrieve, or view obscene, profane, or indecent materials. "Indecent materials" are those materials which, in context, depict or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.

3. Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulation or District policy or rules. This includes, but is not limited to, plagiarism; improper use of copyrighted material; improper use of the System to commit fraud, or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number, of any student, District employee, or System user.
4.
5. Disable or otherwise modify any technology protection measures. Such action shall be the responsibility of the Technology Director or designated representatives for "bona fide research or other lawful purpose".

6. Transfer any software to or from the System without authorization from the System administrator.

7. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.

8. Harass, threaten, intimidate, or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation.

9. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.

10. Disrupt or interfere with the System.

11. Gain unauthorized access to or vandalize the data or files of another user.

12. Gain unauthorized access to or vandalize the System, or the computer system of any individual or organization.

13. Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password.

14. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.

15. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.

16. Send nuisance electronic mail or other online messages, such as chain letters, pyramid schemes, or obscene, harassing, or other unwelcome messages.

17. Send mass electronic mail to multiple users without prior authorization by the appropriate District administrator.

18. Conceal or misrepresent the user's identity while using the System.

19. Post material on the District's web site.

D. Disclaimer

The District makes no warranties of any kind whether express or implied for the System. The District will not be responsible for any damages incurred including the loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. Use of any information obtained via the System is at the user's own risk. The District denies any responsibility for the accuracy or quality of information obtained through the System. The District is not responsible for any user's intentional or unintentional access of material on the Internet which may be obscene, indecent, or of an inappropriate nature.

E. Security and User Reporting Duties

Security in the System is a high priority and must be a priority for all users. Users are prohibited from sharing their login ID or password with any other individual. Any attempt to log in as another user will result in immediate consequences as set forth in Section G of these Guidelines.

A user who becomes aware of any security risk or misuse of the System must immediately notify the supervising District employee.

F. Vandalism

Vandalism or attempted vandalism to the System is prohibited and will result in immediate consequences as set forth in Section G of these Guidelines, and in potential legal action. Vandalism includes, but is not limited to, the downloading, uploading, or creating computer viruses.

G. Consequences for Violations

A user of the District Computer System who engages in any of the prohibited acts listed above shall be subject to consequences which may include the denial, suspension or revocation of System privileges as set forth in these Guidelines and the District's policies, and referral to law enforcement agencies or other legal action in appropriate cases.

AUTHORIZATION FOR ACCESS TO DISTRICT COMPUTER SYSTEM BY STUDENTS

By signing this Authorization, I acknowledge that I have received a copy of the "Guidelines for Acceptable Use of District Computer System by Students" dated April 11, 2007, and that I have read, understand, and agree to follow the Guidelines.

I acknowledge that access to the District Computer System is provided as a privilege by the District and that inappropriate use may result in discipline.

I ACKNOWLEDGE THAT I HAVE NO EXPECTATION OF PRIVACY IN MY USE OF THE DISTRICT COMPUTER SYSTEM, AND THAT THE DISTRICT HAS THE RIGHT TO AND DOES MONITOR USE OF THE SYSTEM.

Student Name: _____ Grade: _____

Student Signature:_____ Date: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____ Date: _____

The "District Computer System Use and Internet Safety Policy" and "Guidelines for Acceptable Use of District Computer System by Students" must be read and thi Authorization for Access must be signed by each student (and if under age 18 by his/her parent/guardian) as a condition of using the District Computer System.

AUTHORIZATION FOR ACCESS TO DISTRICT COMPUTER SYSTEM BY EMPLOYEES

By signing this Authorization, I acknowledge that I have received a copy of the "Guidelines for Acceptable Use of District Computer System by Employees" dated April 11, 2007 and that I read, understand, and agree to follow the Guidelines.

Any user of the system who knowingly and purposefully engages in any of the prohibited acts as listed in the Guidelines shall be subject to disciplinary consequences.

I ACKNOWLEDGE THAT I HAVE NO EXPECTATION OF PRIVACY IN MY USE OF THE DISTRICT COMPUTER SYSTEM, AND THAT THE DISTRICT HAS THE RIGHT TO AND DOES MONITOR USE OF THE SYSTEM.

Name: _____

Signature: _____

Date: _____

The "District Computer System Use and Internet Safety Policy" and "Guidelines for Acceptable Use of District Computer System by Employees" must be read and this Authorization for Access must be signed by each user as a condition of using the District Computer System.

AUTHORIZATION FOR ACCESS TO
DISTRICT COMPUTER SYSTEM BY COMMUNITY MEMBERS

This form must be read and signed by each user of the District Computer System (and if under 18 by his/her parent/guardian) as a condition of using the System.

By signing this Authorization, I acknowledge that I have received a copy of the "Guidelines for Acceptable Use of District Computer System by Community Members," dated April 11, 2007 and that I read, understand, and agree to follow the Guidelines.

I understand that the District makes no warranties with respect to the District Computer System, and specifically that it assumes no responsibility for any cost, liability, or damages for an individual's use of the System, or for any retrieval of or access to illegal, obscene, or indecent material or information.

I ACKNOWLEDGE THAT I HAVE NO EXPECTATION OF PRIVACY IN MY USE OF THE DISTRICT COMPUTER SYSTEM, AND THAT THE DISTRICT HAS THE RIGHT TO AND DOES MONITOR USE OF THE SYSTEM.

User Name: _____ Age: _____

User Signature: _____ Date: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____ Date: _____
(Parent/Guardian signature required if user is under age 18)

The "District Computer System Use and Internet Safety Policy" and "Guidelines for Acceptable Use of District Computer System by Community Members" must be read and this Authorization for Access must be signed by each user of the District Computer System (and if under 18 by his/her parent/guardian) as a condition of using the System.