Uniontown Area School District
Internet Safety,
Acceptable Use,
and
Technology Policy

April 12, 2005

Acceptable Use of District Technology

To better serve our students and provide our employees with the best tools to do their jobs, the District makes available to our students and staff access to one or more forms of electronic media and services, including computers, video devices, music playback devices, copiers, networks, e-mail, the Internet and the World Wide Web. The District has in place certain measures that are meant to shield users from unintentional transgressions. Among these is our firewall that prevents anyone without a signed AUP from accessing the Internet. Along with this safeguard is content filtering through Surf Control as specified in the Federal Government's Children's Internet Protection Act. The intent of CIPA is to block Internet sites that contain visual depictions that are "obscene", "child pornography", and "harmful to minors." Measures designed to restrict minors' access to material "harmful to minors" includes, but is not limited to, using filtering to restrict: gambling, violence, hate speech, criminal skills, weapons, chat, and adult/sexually explicit sites and topics. The filter can be temporarily relaxed for an adult for "bona fide research or other lawful purposes." This would be done on a case-by-case basis and would be reviewed by the building principal and the Technology Coordinator. This access would be only for the time needed to complete the research.

Monitoring the online activities of minors and staff on the Internet is accomplished through teacher supervision, the ability to monitor real-time activity, and the scanning of filter and firewall logs by district personnel. As part of the technology curriculum students are instructed on Internet safety including but not limited to: safety and security when using electronic mail, chat rooms, instant message services, other forms of direct electronic communications, unauthorized access, including so-called 'hacking' and other unlawful activities. These topics are also addressed later in this policy. While using the District computers and network, chat rooms, instant messaging services and other forms of direct electronic communications are restricted.

Individuals will be granted access to technology and services appropriate for their educational needs and goals. **Access to these resources is a privilege not a right and the District has the right to restrict or remove access at any time when violations occur.** The district technology resources are established for the purposes of communication and data sharing in support of educational goals. The District encourages use of these devices and media because they can make communication more efficient and effective. Also they are valuable tools and sources of information for students and staff. However, all employees, students, and anyone connected to the organization should remember that devices and media provided by the District are District property. Their purpose is to facilitate and support the District's curriculum and educational mission. **The use of equipment, media or services for purposes that do not support the educational mission and curriculum of the District is prohibited. Misuse or destruction of the equipment is prohibited. <u>All users</u>** have the responsibility to use these resources in a lawful, professional, and ethical manner

To help ensure that all employees and students act in a responsible manner the following security and safety guidelines have been established for using district and personal technology and media. No policy can lay down rules to cover every possible situation. Instead it is designed to express the District's philosophy and set forth, general principles for using electronic devices, media and services.

Users shall only use the account and/or password assigned to them, unless they are assigned multiple accounts.

Prohibited Activities:

- Use of the District technology for non-work or non-school related communications or projects are prohibited. Limited occasional or incidental use of electronic media (sending and receiving) for personal purposes is understandable and acceptable. All such use should be done in a manner that does not negatively affect the systems' use for their educational purposes. However employees and students are expected to demonstrate a sense of responsibility and not abuse this privilege.
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors or staff.
- The District technology shall not be used to disrupt the work of others: and the hardware or software or files of other users shall not be destroyed, modified or abused in any way.
- Using technology that results in any copyright violation is prohibited.
- Use of technology for malicious purposes; harassment of others, infiltrating computer systems, and/or damaging computers, software, or other technology device is prohibited.
- Use of the District technology to intentionally obtain or modify files, passwords, or data belonging to other users is prohibited.
- Attempting to disguise your account or machines identity is prohibited.
- No user may attempt to circumvent security or data protection.
- Deliberately wasting or monopolizing resources is prohibited. This includes but is not limited to subscribing to list servers, mass emailing, Internet games, or creating unnecessary network traffic.

Electronic devices, media and services cannot be used for knowingly transmitting, retrieving, or storing and communication that is:

1. Discriminatory or harassing:
2. Derogatory to any individual or group:
3. Obscene, sexually explicit or pornographic:
4. Defamatory or threatening:
5. In violation of any license covering the use of software:
6. Used for product advertising or used for political opinions and / or lobbying.
7. Engage in for any purpose that is illegal or contrary to the District policy or interests.
8. Causing damage to or changing function, operation, or design of the technology.

SCHOOL OWNED EQUIPMENT:

Computers: This includes but is not limited to; workstations and notebook computers and PDA's Tampering with, vandalism to, or unauthorized use of this equipment is prohibited. Use of these devices for activities other than those directly related to the curriculum or mission of the district is prohibited. Violation of this policy will result in disciplinary actions, and violators may be subject to serious criminal prosecution.

Peripherals: This includes but is not limited to; printers, scanners, Smart Boards, and storage devices. Tampering with, vandalism to, or unauthorized use of this equipment is prohibited.

Use of these devices for activities other than those directly related to the curriculum or mission of the district is prohibited. Violation of this policy will result in disciplinary actions, and violators may be subject to serious criminal prosecution.

Copiers: This includes but is not limited to school owned copying devices. These devices are to be used for educational purposes. Use of these devices for activities other than those directly related to the curriculum or mission of the district is prohibited. Personal use is prohibited. Users are prohibited from making copies of copyrighted materials in violation of copyright and / or Fair Use laws and guidelines.

Video Devices: This includes but is not limited to; Televisions, VCRs, DVD players, video projectors, digital cameras, digital camcorders, and video recorders. Tampering with, vandalism to, or unauthorized use of this equipment is prohibited. Use of these devices for activities other than those directly related to the curriculum or mission of the district is prohibited. Violation of this policy will result in disciplinary actions, and violators may be subject to serious criminal prosecution. Users are prohibited from making copies of copyrighted materials in violation of copyright and / or Fair Use laws and guidelines.

Musical playback / recording equipment: This includes but is not limited to; radios, CD players, cassette player / recorders. Tampering with, vandalism to, or unauthorized use of this equipment is prohibited. Use of these devices for activities other than those directly related to the curriculum or mission of the district is prohibited. Violation of this policy will result in disciplinary actions, and violators may be subject to serious criminal prosecution. Users are prohibited from making copies of copyrighted materials in violation of copyright and / or Fair Use laws and guidelines.

Calculators: Calculators used that are the property of the school district are not to be tampered with or vandalized in any way. Personal calculators are permitted as long as their use is related to school activities. Violations of this rule will result in disciplinary actions.

Id cards: No one can use another person's ID card for any reason. No one should allow anyone to use his or her card. Violation of this policy will result in disciplinary actions, and violators may be subject to serious criminal prosecution.

SOFTWARE:

Users will not copy or install personal software onto the network or onto any hard drive of a computer; either stand-alone or connected to the network. Users will not use any personal software from a floppy disk, zip disk, CD-ROM, or other portable media. It is prohibited to provide copies of copyrighted software to others while maintaining personal copies, unless there is a specific provision in the copyright policy allowing such action. Using a copyrighted program on more that one machine is prohibited, unless the copyright provision allows such an action. The district will not allow the illegal use of software. Violation of this policy will result in disciplinary actions. Loading or use of unauthorized games, programs, music, files or other electronic media is prohibited.

Communications Software: This includes but is not limited to; Email, messaging, or chat. Users are not to engage any type of messaging or chat during school hours. Email communication other than that required for educational activities (distance learning, collaboration, etc.) is prohibited. Violation of this policy will result in disciplinary actions, and violators may be subject to serious criminal prosecution.

Productivity, Curriculum, Network Software: This software is to be used as designated in the curriculum and to aid in the instruction of students. Use of this software for uses other than those directly related to the curriculum and mission of the district is prohibited.

Management: This software is to be used to manage the information required for the operation of the school district. District, State and Federal privacy and confidentiality rules apply to all data contained in the system. Only the student, parents or guardians, and school personnel directly involved in the student's education, attendance, health, and discipline may view data concerning a student. Use of this software for uses other than those stated above is prohibited.

Responsibility for Data: Although every effort is made to prevent the loss of user data using hardware redundancy and backup strategies, the District assumes no responsibility for user data that is lost or destroyed due to software or hardware failures.

This policy is designed for all students and employees of the District. Find the Level to which you are associated to review the specific technology guidelines.

LEVEL 1 USER:

This group includes but is not limited to **STUDENTS, Part Time Employees (Security, Secretarial, Cafeteria and Custodial Staff)** and others assigned to this group by school district administration.

ACCESS TO DATA / DATA INTEGRITY:

All data stored on district equipment is the property of the district.

- Users at this level are to access their personal files and any data files that are required for their class or homework assignments or job.
- Access to other files without permission is expressly forbidden.
- Reading or altering any file that has not been designated for your use is a violation of this policy. **Users will not reveal their password to others or access unauthorized data with another user's password.**

PERSONAL ELECTRONIC DEVICES:

Computers: This includes but is not limited to: workstations, laptops and handheld PC's. These items are not allowed in school unless directly involved in a sanctioned educational activity.

Communications Devices: This includes but is not limited to; pagers, cellular phones, and PDA's. These devices are prohibited from use during the time school is in session. There are no school-sanctioned activities where these devices may be used. Violation of this rule will result in disciplinary action as outlined in the student handbook and/ or contract. {C*ellular phones and other electronic devices are not permitted on school grounds while school is in session and during any school sponsored activity including transportation. Violators will be suspended / expelled. Electronic devices that have been confiscated will only be released to a parent or guardian.*}

Music playback/recording devices: This includes but is not limited to; CD players, cassette player / recorders, MP3 players, and radios. These items are not allowed in school unless directly involved in a sanctioned educational activity.

LEVEL 2 USER:

This group includes but is not limited to **Teachers, Full-time Secretarial Staff, Guidance Counselors, Designated Buildings and Grounds Staff** and others assigned to this group by school district administration. Users at this level are responsible for District equipment used in their classes or for their duties. This includes but is not limited to: computers, notebook computers, portable labs, audio and video equipment, and SmartBoards™.

ACCESS TO DATA:

All data stored on district equipment is the property of the district.

- Users at this level are to access their personal files and any data files that are required to perform their stated job functions as assigned by their supervisor.
- Access to other files without permission is expressly forbidden. Reading or altering any file that has not been designated for your use is a violation of this policy.
- All data entered should be checked and verified for accuracy. Users are responsible for errors in entering verified data.
- The highest level of accuracy is required when entering data in District Information Systems. Intentionally entering false or erroneous data is grounds for immediate disciplinary action by the district. Local, state and federal law enforcement could be notified based on the scope of the infraction.
- All data entered and viewed is subject to District and state privacy and confidentiality policies.
- Users will not reveal their password to others or access unauthorized data with another users password.

PERSONAL ELECTRONIC DEVICES:

Computers: This includes but is not limited to: workstations, laptops and handheld PC's. These devices are prohibited from use during student instructional time, except for a classroom emergency. They may be used during planning or lunch periods as long as students are not present. Violation of this rule will result in disciplinary action as outlined in the contract. Any such devices will not be serviced or repaired by the District. No network connection will be provided.

Communications Devices: This includes but is not limited to; pagers, cellular phones, and PDA's. These devices are prohibited from use during student instructional time, except for a classroom emergency. They may be used during planning or lunch periods as long as students are not present. Violation of this rule will result in disciplinary action as outlined in the contract.

Music playback/recording devices:
This includes but is not limited to; CD players, cassette player / recorders, MP3 players, and radios. These items are not allowed in school unless directly involved in a sanctioned educational activity.

LEVEL 3 USER:

This group includes but is not limited to **Administrative Staff, Building Principals, Supervisors,** and others assigned to this group by school district administration.

ACCESS TO DATA:

All data stored on district equipment is the property of the district.

- Users at this level are to access their personal files and any data files that are required to perform their stated job functions as assigned by their supervisor.
- Access to other files without permission is expressly forbidden. Reading or altering any file that has not been designated for your use is a violation of this policy.

- All data entered should be checked and verified for accuracy. Users are responsible for errors in entering verified data.
- The highest level of accuracy is required when entering data in District Information Systems. Intentionally entering false or erroneous data is grounds for immediate disciplinary action by the district. Local, state and federal law enforcement could be notified based on the scope of the infraction.
- All data entered and viewed is subject to District and state privacy and confidentiality policies.
- Users will not reveal their password to others or access unauthorized data with another users password.

PERSONAL ELECTRONIC DEVICES:

Computers: This includes but is not limited to: workstations, laptops and handheld PC's. These devices are prohibited from use during student instructional time, except for a classroom emergency. They may be used during planning or lunch periods as long as students are not present. Violation of this rule will result in disciplinary action as outlined in the contract. Any such devices will not be serviced or repaired by the District. No network connection will be provided.

Communications Devices: This includes but is not limited to; pagers, cellular phones, and PDA's. These devices are prohibited from use during student instructional time, except for a classroom emergency. They may be used during planning or lunch periods as long as students are not present. Violation of this rule will result in disciplinary action.

Music playback/recording devices:
This includes but is not limited to; CD players, cassette player / recorders, MP3 players, and radios. These items are not allowed in school unless directly involved in a sanctioned educational activity.

LEVEL 4 USER: This group includes but is not limited to **Administrative Technology Staff,** and others assigned to this group by school district administration.

Only Technology Staff is authorized to service or repair hardware, install or remove software, and create accounts, install file servers, and other network devices.
Users at this level have access to technology and data based on their job requirements. They are not to view files not directly related to assist users, maintenance, security, and affirmation of policy compliance.

ACCESS TO EMPLOYEE AND STUDENT COMMUNICATIONS

Generally, electronic information created and/or communicated by an employee or student using e-mail, word processing, utility programs, spreadsheets, Internet and bulletin board system access, and similar electronic media; is not continuously reviewed by the District. However, the following conditions should be noted:

The District does routinely gather logs for most electronic activities or monitor student / employee communications directly, e.g., files accessed, sites accessed, access length, and time at which access is made, for the following purposes:

1. Cost analysis;
2. Resource allocation;
3. Optimum technical management of information resources: and
4. Detecting patterns of use that indicate employees or students are violating District policies or engaging in illegal activity.

The District reserves the right, at its discretion, to review any employee's or student's electronic files and messages to the extent necessary to ensure district technology and services are being used in compliance with the law, this policy and other District policies.

CONSEQUENCES FOR INAPPROPRIATE USE

- The user regardless of level shall be responsible for damages to the equipment, systems, or software resulting from deliberate or willful acts.
- Failure to follow the procedures and prohibitions listed above may result in the loss of the right of access to the District network, computer equipment, or the Internet. Other appropriate disciplinary procedures may take place as needed, for students and employees.
- Illegal use of District equipment; intentional deletion or damages to files will be reported to the appropriate legal authorities for possible prosecution.
- All agreements and regulations that apply shall determine the level of discipline. These include but are not limited to the Student Handbook, the Faculty Handbook, contracts, service agreements, Codes of Conduct, Local, State and Federal laws and regulations.

District Acceptable Technology Use Agreement

As a user of the District, I hereby acknowledge that I have read and understand the District's policy in regard to my access and use of the District Technology and the Internet. I agree to comply with that policy in regard to my access and use of the District's Technology and the Internet. I understand that my failure to abide by the District's policy on the subject will result in the loss of my privilege to access and use the District's technology and/or the Internet, and that more serious violations may result in other disciplinary or legal action.

Please check the box represents your user level:

☐ Level I ☐ Level II ☐ Level III ☐ Level IV

_____
School

_____ _____
User's Name (Please Print) Username

_____ _____
Date User's Signature

DISTRICT PARENTAL PERMISSION FORM
To be completed by the Parent or Guardian of Students

To be completed ONLY by parent/legal guardian who wishes to permit student INTERNET use.

As the parent/legal guardian of _____, I hereby acknowledge that I have read and understand the policy of the District in regard to a student's use of the Internet, and hereby grant permission for said student to use the school's technology and to access the Internet.

_____ _____ _____
Date Phone Signature of Parent/Guardian

PARENTAL REQUEST TO DENY ALL TECHNOLOGY USE
To be completed ONLY by parent/legal guardian who wishes to <u>RESTRICT ALL STUDENT TECHNOLOGY USE.</u>

As the parent/legal guardian of _____, I hereby request that the District restrict all use of District Technology for this student.

_____ _____ _____
Date Phone Signature of Parent/Guardian