No. 815

SECTION: OPERATIONS
TITLE: ACCEPTABLE USE POLICY FOR COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND DIGITAL INFORMATION

ADOPTED: February 10, 1998

REVISED: October 9, 2001
July 12, 2005

Upper Dauphin Area School District

815. ACCEPTABLE USE POLICY FOR COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND DIGITAL INFORMATION

1. Purpose

It is the goal of the Upper Dauphin Area School District (UDASD) to prepare students to become computer literate in an increasingly technological world. In fulfillment of this mission, UDASD provides employees, students, and guests (users) with access to the UDASD electronic communication systems and network, which includes computer software, curriculum resources, and Internet access, whether wired or wireless, or by any other means

Computers, network, Internet, electronic communications, and information systems (collectively "CIS systems") provide vast, diverse and unique resources. UDASD provides access to the CIS systems for employees, students, and the community to access information, research, to facilitate learning and teaching, and to foster the educational purpose and mission of the UDASD.

For all users, the UDASD CIS systems must be used primarily for education related purposes and performance of UDASD job duties. Incidental personal use of school computers is permitted for employees as defined in "Definitions" below. Personal use must comply with this policy and all other applicable UDASD policies, procedures, and rules contained in this policy, as well as Internet service provider (ISP) terms, local, state and federal laws and must not damage the UDASD CIS systems. All users' personal technology devices brought onto UDASD property or

suspected to contain UDASD information may be legally accessed to insure compliance with this Policy and other UDASD policies to protect the UDASD resources, and to comply with the law. Users may not use their personal property to access the School District's network, Internet or any other CIS System unless approved by the UDASD administration.

The UDASD intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical in protecting these UDASD assets and in lessening the risks that can destroy these important and critical assets. Consequently, guests, employees, and students are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the UDASD administration,. Conduct otherwise will result in actions further described in Section 16 – Consequences for Inappropriate, Unauthorized, and Illegal Use, found as the last Section of this Policy, and as provided in other relevant UDASD policies.

2. Definitions

Access to the Internet

A computer shall be considered to have access to the Internet if the computer is connected to a network that has access to the Internet, whether by wire, wireless, cable, or any other means.

Child Pornography

Any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

b. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

c. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Computer

Includes any UDASD owned, leased or licensed, or employee, student and guest owned personal hardware, software, or other technology used on UDASD premises or at UDASD events, or connected to the UDASD network, containing UDASD programs or UDASD or student data

(including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a computer. "Computer" includes, but is not limited to, UDASD, employee, students, and guest: desktop, notebook, powerbook, tablet PC or laptop computers, printers, cables, modems, and other peripherals; specialized electronic equipment used for students' special educational purposes; global position system (GPS) equipment; personal digital assistants (PDAs), cell phones, with or without Internet access and/or recording and/or camera and other capabilities, mobile phones, or wireless devices, beepers, paging devices, computer driven telescopes, and two-way radios/telephones, laser pointers and attachments, and any other such technology developed.

Discriminatory Material

Depicting a bias against individuals as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability.

Electronic Communications Systems

Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an electronic communications system means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage or such communications. Examples include, but are not limited to, the Internet, intranet, electronic mail services, Global Positioning Systems, Personal Digital Assistants, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras, and other capabilities.

Educational Purpose

Includes use of the CIS systems for classroom activities, professional or career development, and to support the UDASD curriculum, policy, and mission statement.

Harmful to Minors

Any picture, image, graphic image file or other visual depictions that:

a. taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;

b. depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals, and

c. taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

Incidental Personal Use

Use of UDASD CIS systems by an individual for occasional personal research and communications. Personal use must comply with this policy and all other UDASD policies, procedures and rules, as well as ISP, local, state, and federal laws and may not interfere with the user's job duties and performance, with system operations, or with other system users, and must not damage the UDASD CIS systems. Under no circumstances should a user believe their use is private. The UDASD reserves the right to monitor, track, access, and log the use of its CIS systems at any time.

Inappropriate Matter

Includes, but is not limited to, visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory, violent, bullying, terroristic, and advocates the destruction of property.

Minor

For purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean the age of minority as defined in the relevant law.

Network

A system that links two or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, software, and other computers and/or networks to which the UDASD network may be connected, such as the Internet, the Internet2, or those of other institutions.

Obscene

Analysis of the material meets the following elements:

a. whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;

b. whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene; and

c. whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

Sexual Act and Sexual Contact

As defined at 18 U.S.C. § 2246 (2), and at 18 U.S.C. § 2246 (3), 18 Pa. C.S.A. § 5903.

Technology Protection Measure (s)

A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.

Visual Depictions

Undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.

3. Authority

Access to the UDASD CIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the UDASD, which reserves the right to deny access to prevent further unauthorized, inappropriate, or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The UDASD will cooperate to the extent legally required with the ISP, local, state, and federal officials in any investigation concerning or related to the misuse of the CIS systems.

It is often necessary to access user accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users have

no privacy expectation in the contents of their personal files or any of their use of the UDASD CIS systems. The UDASD reserves the right to monitor, track, log, and access CIS systems use and to monitor and allocate fileserver space.

The UDASD has the right to lock the storage media on individual computers using hardware or software technology to prevent unauthorized tampering with computer configuration and/or the loading of unauthorized software.

The UDASD reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the UDASD operates and enforces technology protection measures that block or filter online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. Measures designed to restrict user access to material harmful to minors may be disabled to enable an adult to access *bona fide* research or for another lawful purpose.

The UDASD has the right, but not the duty, to monitor, track, log, access, and report all aspects of its computer information technology and related systems of all users and of any employee's, student's and guest's personal computers, network, Internet, electronic communication systems, and media brought on to UDASD premises or at UDASD events, connected to the UDASD network, containing UDASD programs or UDASD or student data (including images, files, and other information) to insure compliance with this policy and other UDASD policies, to protect the UDASD resources, and to comply with the law.

The UDASD additionally reserves the right to:

a. Determine which CIS systems services will be provided through UDASD resources.

b. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.

c. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time.

d. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable UDASD policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of UDASD resources and equipment.

4. Responsibility

Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, discriminatory, inaccurate, obscene, sexually explicit, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, profane, pornographic, offensive, and illegal, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the UDASD cannot completely block assess to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in actions explained further in Section 16 Consequences for Inappropriate, Unauthorized, and Illegal Use, found in the last Section of this policy and as provided in relevant UDASD policies.

Employees must become proficient in the use of the UDASD CIS systems, and software relevant to the employee's responsibilities and practice proper etiquette, ethical behavior, and agree to the requirements of this policy. 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 abrasive in messages to others. General UDASD rules and policies for behavior and communicating apply.

b. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.

c. Do not reveal the personal addresses or telephone numbers of other users.

d. Recognize that e-mail is not private or confidential.

e. Do not use the internet or e-mail in any way that would interfere with or disrupt its use by other users.

f. Consider all communications and information accessible via the internet to be the property of the UDASD.

g. Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital status, or handicap status.

5. Delegation of Responsibility

The UDASD will serve as the coordinator to oversee the UDASD CIS systems and will work with other regional or state organizations as necessary, to educate employees, approve activities, provide leadership for

proper training for all users in the use of the CIS systems and the requirements of this policy, establish a system to insure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy.

The UDASD Administration and/or designee will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, and establish the UDASD virus protection process.

Unless otherwise denied for cause, student access to the CIS systems resources shall be through supervision by the professional staff. Administrators, teachers, and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within the UDASD CIS systems, and to abide by the rules established by the UDASD.

6. Guidelines

1. Access to the CIS Systems

CIS systems user accounts will be used only by authorized owners of the accounts for authorized purposes.

An account will be made available according to procedures developed by appropriate UDASD authorities.

2. CIS Systems

The UDASD Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Policy, as well as other relevant UDASD policies, will govern use of the UDASD CIS systems for students, employees, and guests. Use of the CIS systems will also be governed by the other relevant UDASD policies, and where applicable, school district policies in which the CIS systems are located.

Types of Services included, but not limited to:

World Wide Web. UDASD employees, students, and guests will have access to the Web through the UDASD CIS systems as needed.

E-Mail. UDASD employees may be provided assigned individual e-mail accounts for work related, and incidental personal use, as needed.

Guest Accounts. Guests, which include but are not limited to, visitors, workshop attendees, volunteers, independent contractors, and adult education instructors, may receive an individual account

with the approval of the UDASD Administration if there is a specific, UDASD-related purpose requiring such access. Use of the computers, network, and internet by a guest must be specifically limited to the UDASD-related purpose. An agreement will be required and parental signature will be required if the guest is a minor.

Access to all data on, taken from, or compiled using UDASD computers is subject to inspection and discipline. Users have no right to expect that UDASD information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the UDASD. The UDASD reserves the right to legally access users' personal equipment for UDASD information.

3. Parental Notification and Responsibility

The UDASD will notify the parents about the UDASD CIS systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the UDASD to monitor and enforce a wide range of social values in student use of the Internet. Further, the UDASD recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The UDASD will encourage parents to specify to their child (ren) what material is and is not acceptable for their child (ren) to access through the UDASD CIS system. Parents are responsible for monitoring their children's use of the UDASD CIS systems when they are accessing the systems.

4. UDASD Limitation of Liability

The UDASD makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the UDASD CIS systems will be error-free or without defect. The UDASD does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the UDASD, nor is the UDASD responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The UDASD shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, mis-delivered, or unavailable when using the computers, network and electronic communications systems. The School District will not be responsible for stolen, damaged, or lost personal devices of students, employees, contractors, and guests. The UDASD shall not be responsible for material that is retrieved through the Internet, or the consequences that may result

from them. The UDASD shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the UDASD CIS systems. In no event shall the UDASD be liable to the user for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems.

5. Prohibitions

The use of the UDASD CIS systems for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited and illustrated in Section 6 below.

The UDASD reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS systems.

These prohibitions are in effect any time UDASD resources are accessed whether on UDASD property, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee, student, or guest uses their own equipment.

Students are prohibited from visibly possessing and using their personal computers, as defined in this policy, on UDASD premises and property (including but not limited to, buses and other vehicles), at UDASD events, or through connection to the UDASD CIS systems, unless expressed permission has been granted by a teacher or administrator, who will then assume the responsibility to supervise the student in its use, or, unless an IEP team determines otherwise, in which case, an employee will supervise the student in its use.

Students who are performing volunteer fire company, ambulance, or rescue squad functions, or need such a computer due to their medical condition, or the medical condition of a member of their family, with notice and the approval of their family, with notice and the approval of the school administrator may qualify for an exemption of this prohibition.

6. General Prohibitions

Users are prohibited from using UDASD CIS systems to:

- Communicate about non-work or non-school related communications unless such use comports with this policy's definition or incidental personal use.

- Access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.
- Access or transmit material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic, and/or illegal.
- Bully another individual.
- Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other betting or games of chance.
- Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.
- Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.
- Participate in unauthorized Internet Relay Chats, instant messaging communications, and Internet voice communications (on-line; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.
- Communicate through e-mail for non-educational purposes or activities, unless it is for an incidental personal use as defined in this policy. The use of e-mail to mass mail non-educational or no-work related information is expressly prohibited (for example, the use of the "everyone" distribution list, building level distribution lists, or other e-mail distributions lists to offer personal items for sale is prohibited).
- Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable UDASD policies); conduct unauthorized fund raising or advertising on behalf of the UDASD or use the UDASD name in any unauthorized manner that would reflect negatively on the UDASD, its employees, or students.
- Engage in political lobbying.
- Install, distribute, reproduce or use copyrighted software on UDASD computers, or copy UDASD software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.

- Install computer hardware, peripheral devices, network hardware, or system hardware. The authority to install hardware or devices on UDASD computers in restricted to the UDASD Administration or designee.
- Encrypt messages using encryption software that is not authorized by the UDASD from any access point on UDASD equipment or UDASD property. Employees and students must use UDASD approved encryption to protect the confidentiality of sensitive or critical information in the UDASD approved manner.
- Access, interfere, possess, or distribute confidential or private information without permission of the School District administration. An example includes accessing student accounts to obtain their grades.
- Violate the privacy or security of electronic information.
- Use the systems to send any UDASD information to another party, except in the ordinary course of business as necessary or appropriate.
- Send unsolicited commercial electronic mail messages, also known as spam.
- Post personal or professional web pages without administrative approval.
- Post anonymous messages.

7. Access and Security Prohibitions

Users must immediately notify the UDASD Administration and/or designee if they have identified a possible security problem. Students, employees, and guests must read, understand, provide signed acknowledgment form and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure, and physical information security policies. The following activities related to access to the UDASD CIS systems are prohibited:

- Acquiring or attempting to acquire passwords of others or giving your password to another. Users will be held responsible for the result of any misuse of the users' user name or password while the users' systems access were left unattended and accessible to others, whether intentional or through negligence.
- Altering a communication originally received from another person or computer with the intent to deceive.
- Using UDASD resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for the promotion of or the sale of drugs, alcohol, or weapons, engaging in criminal activity, or being involved in a terroristic threat against any person or property.

- Disabling or circumventing any UDASD security, program or device, for example, but not limited to, anti-spyware, anti-spam software, media locking, and virus protection software or procedures.
- Transmitting electronic communications anonymously or under an alias unless authorized by the UDASD.

8. Operational Prohibitions

The following operational activities and behaviors are prohibited:

- Interference with or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", trojan Horse and trapdoor program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. The user may not hack or crack the network or others' computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, or any component of the network, or strip or harvest information, or completely take over a person's computer.
- Altering or attempting to alter files, system security software, or the systems without authorization.
- Unauthorized scanning of the CIS systems for security vulnerabilities.
- Attempting to alter any UDASD computing or networking components (including, but not limited to fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.
- Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, or by other means.
- Connecting unauthorized hardware and devices to the CIS systems.
- Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files.
- Intentionally damaging or destroying the integrity of UDASD electronic information.
- Intentionally destroying a UDASD computer or equipment.
- Intentionally disrupting the use of the CIS systems.
- Damaging the UDASD CIS systems, networking equipment through negligence or deliberate act.

- Failure to comply with requests from appropriate teachers or UDASD administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

9. Content Guidelines

Information electronically published on the UDASD CIS systems shall be subject to the following guidelines:

- Published documents including but not limited to physical depictions, audio and video clips or conferences, may not include a minor's phone number, street address, or box number, name (other than first name) or the names of other family members without parental consent.
- Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.
- Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.
- Documents, web pages, and electronic communications, must conform to all UDASD policies and guidelines, including the copyright policy.
- Documents to be published on the Internet must be edited and approved according to UDASD procedures prior to publication.

10. Due Process

The UDASD will cooperate with the UDASD ISP, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the UDASD CIS systems.

If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights.

The UDASD may terminate the account privileges of any user.

11. Search and Seizure

Users' violations of this Policy, any other UDASD policy, or the law may be discovered by routine maintenance and monitoring of the UDASD system, or any method stated in this policy, or pursuant to any legal means.

The UDASD reserves the right to monitor, track, log, and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason. Users should have no expectation of privacy in their use of the UDASD CIS systems, and other UDASD technology, even when used for personal reasons. Further, the UDASD reserves the right, but not the obligation, to access any personal technology device of users brought onto the UDASD premises or at UDASD events, or connected to the UDASD network, containing UDASD programs or UDASD or student data (including images, files, and other information) to insure compliance with this policy and other UDASD policies, to protect the UDASD resources, and to comply with the law.

Everything that users place in their personal files should be written with no expectation of privacy and under the assumption that a third party will review personal files.

Pol. 94-553
Sec. 107
Pol. 814

12. Copyright Infringement and Plagiarism

Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the UDASD resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements. Employees will respect and comply as well.

Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The UDASD does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.

Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the UDASD computers is expressly prohibited. This includes all forms of licensed software.

UDASD guidelines on plagiarism will govern use of material accessed through the UDASD CIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

13. Selection of Material

Board policies on the selection of materials will govern use of the UDASD CIS systems.

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

14. UDASD Web Site

The UDASD will establish and maintain a Web Site and will develop and modify its Web pages that will present information about the UDASD under the direction of the UDASD Administration. Publishers must comply with the UDASD Web Site Development Policy.

15. Safety & Privacy

To the extent legally required, users of the UDASD CIS systems will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening communications may take them to the UDASD Administration and/or designee.

Users will not post personal contact information about themselves or other people on the CIS systems. The user may not steal another's identity in any way, may not use spyware, parasiteware, cookies, or use UDASD or personnel employee technology or resources in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate confidential and personal information about students or employees (examples include, but are not limited to, using a cell phone with camera and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the UDASD, saving, storing and sending the image with or without text or disclosing them by any means, including but not limited to, print and electronic matter; revealing student grades, social security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the UDASD unless legitimately authorized to do so).

Student users will agree not to meet with someone they have met online unless they have parental consent.

16. Consequences for Inappropriate, Unauthorized, and Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, or for unlawful use of the CIS systems may result in loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions (with or without pay for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant UDASD policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policy, curriculum policies, terroristic threat policy, and harassment policies.

The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.

Violations as described in this policy may be reported to appropriate legal authorities. The UDASD will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to the UDASD CIS systems and resources and is subject to discipline.

SCHOOL DISTRICT RESPONSIBILITIES TO USERS

1. The Upper Dauphin Area School District provides extensive technology assets for use by students, employees, and the community. Access to this technology is a privilege, not a right, and can be revoked from individual users who do not follow these guidelines for acceptable use.

2. Technology assets are to be used primarily for educational purposes, but this policy does make allowances for reasonable incidental personal use such as checking e-mail and doing personal research as long as such personal use does not violate other parts of this policy.

3. The school district will provide electronic storage, user accounts, and e-mail accounts where appropriate for students, employees, and guests.

4. The school district will take reasonable measures to protect users within the district from inappropriate matter as specified by law (U.S. Children Internet Protection Act of 2000 and PA Children Internet Protection Act 197 of 2004).

5. The school district will take reasonable measures to protect users from electronic harassment and unsolicited electronic mail.

6. The District Technology Coordinator will assume responsibility for the development and distribution of Acceptable Use consent forms. The Administrative will maintain signed consent forms for all district employees that are dated no more than one year prior. Individual buildings will maintain signed consent forms for all students and guests. Student consent forms will be updated at the beginning of kindergarten, grade 5, and grade 9. New students enrolling in the district will complete consent forms at registration.

USER RESPONSIBILITIES

1. Users will not attempt to tamper with, relocate, or interfere with the operation of technology assets.

2. Users will not reconfigure computer settings or attempt to load unauthorized software.

3. Users will not abuse technology assets for the purpose of harassing others, accessing inappropriate matter, cheating, plagiarizing, violating copyright, or engaging in illegal activities.

4. Users will not use personal technology items as defined under “Computer” in definitions on school district property unless granted permission to do so under the rules of this policy.

5. Users will report to the UDASD administration any malfunctioning equipment, inappropriate materials discovered, and violations of this policy.

Upper Dauphin Area Elementary School
5668 State Route 209
Lykens, PA 17048

Upper Dauphin Area Middle School
5668 State Route 209
Lykens, PA 17048

Upper Dauphin Area High School
220 North Church Street
Elizabethville, PA 17023

CIS Acknowledgment and Consent Form

Student

I have received, read, and understand this policy and will comply with it. Someone from the UDASD has also reviewed this policy with me and my parents. In addition, I have been given the opportunity to obtain information from the UDASD and my parent(s) about anything I do not understand, and I have received the information I requested. Additionally, I understand that if I violate the policy, I am subject to the UDASD discipline and could be subject to ISP as well as local, state, and federal legal recourse.

Name of Student_____

Signature of Student_____

Date of Signature_____

Parent (s)

As the parent of a student of the UDASD, I have received, read, and understand the Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Policy. In addition, I reviewed this policy with my child and answered questions he or she asked. I agreed to have my child abide by the rules of the policy.

Name of Parent_____

Signature of Parent_____

Date of Signature_____

Upper Dauphin Area School District
5668 State Route 209
Lykens, PA 17048

CIS Acknowledgment and Consent Form

Employee

As an employee of UDASD, I have received, read, and understand this policy and will comply with it. In addition, I reviewed this policy with my students and answered questions they asked. I agree to abide by the rules of the policy.

Name of Employee_____

Signature of Employee_____

Date of Signature_____

Upper Dauphin Area Elementary School
5668 State Route 209
Lykens, PA 17048

Upper Dauphin Area Middle School
5668 State Route 209
Lykens, PA 17048

Upper Dauphin Area High School
220 North Church Street
Elizabethville, PA 17023

CIS Acknowledgment and Consent Form

Guest

As a guest of UDASD, I have received, read, and understand this policy and will comply with it. I agree to abide by the rules of the policy.

Name of Guest_____

Signature of Guest_____

Date of Signature_____