

# UPPER BUCKS COUNTY TECHNICAL SCHOOL

No. 815-AR  
UPPER BUCKS COUNTY  
AREA VOCATIONAL  
TECHNICAL SCHOOL

ADMINISTRATIVE  
REGULATION

Revised May 17, 2012

## **815-AR Upper Bucks County Technical School's Staff Computing and Information Systems User Guidelines**

### Overview

The Acceptable Electronic Technology Use Policy for the School's computing and networked information adopted by the Joint Operating Committee defines the School's position regarding the use of its computing and information systems. The following guidelines are based on that policy and establish standards for acceptable use of all School computers, computer networks, information systems, and Internet connections by staff. These guidelines provide a means by which the Administration will regulate Staff use of the School's computing and information systems.

The Upper Bucks County Technical School's computing and information systems are provided for a specific, limited purpose: to enhance the delivery of education. Consequently, the use of School computing and information systems shall be restricted to educational purposes, i.e., activities directly connected to, and which are a direct result of, the established school curriculum and/or the management of the school. All staff members shall follow all regulations and meet all standards as set forth in this document. Failure to do so may result in loss of access privileges and/or other disciplinary action (see "Consequences").

It is the policy of Upper Bucks County Technical School to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

### Definitions

The terms of this policy are defined as follows:

**Access** - (computer) shall mean, in relation to computers to obtain entry to, or to locate, read into memory, and make ready for some operation.

**Application(s)** - shall mean a software program or group of programs designed for users. Applications shall include either systems software and/or applications software.

**Child pornography** - The term child pornography is defined under both federal and state law.

Under federal law, is 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:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. 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
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.

**Computer(s)** - shall mean desktops, laptops, workstations, servers, PDAs, mobile devices, telephones, tablets, or any other technology device of a similar nature that is owned, leased, or licensed by or to the Upper Bucks County Technical School.

**Harmful to minors** - The term harmful to minors is defined under both federal and state law.

Under federal law, is any picture, image, graphic image file or other visual depiction that:

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
2. 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 contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and
3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;
2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

**Obscene** - any material or performance, if:

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;
2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

**Technology** - all forms of technology that is provided directly or indirectly by the Upper Bucks County Technical School to its users, and that is: (i) owned, leased, or licensed to the Upper Bucks County Technical School; or (ii) that is accessed by or through technology that is owned, leased, or licensed to the Upper Bucks County Technical School.

Technology includes, but is not limited to:

- computers,
- copiers,
- printers,
- scanners,
- electronic portable devices,
- electronic peripheral devices,
- servers,
- networks,
- programs/applications,
- software,
- files,
- folders,
- data and records of any nature,
- the Internet,
- cell phones,
- mobile devices,
- pagers,
- PDAs,
- modems,
- voicemail,
- email,
- chat rooms,
- blogs,
- instant messages,
- videoconferencing,
- user group and such similar technologies.,

#### Access To Inappropriate Material

To the extent practical, technology protection measures (or “Internet filters”) shall

be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

### Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Upper Bucks County Technical School online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

### Education, Supervision and Monitoring

It shall be the responsibility of all members of the Upper Bucks County Technical School staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director and/or his/her designee or designated representatives.

The Palisades School District, Penridge School District and Quakertown Community School District as the home sending districts will provide age appropriate training for students who use the Upper Bucks County Technical School's Internet facilities.

The training provided will be designed to promote the School's commitment to:

- a. The standards and acceptable use of Internet services as set forth in the School's Acceptable Use Policy;
- b. Student safety with regard to:
  - i. safety on the Internet;
  - ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
  - iii. cyberbullying awareness and response.
- c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the

training, understood it, and will follow the provisions of the District's acceptable use policies.

### Responsibilities

The School is responsible for defining reasonable boundaries for acceptable use of the School's computing and informational system(s); educating students, staff and other users about the acceptable uses; providing general supervision; and enforcing the policies for acceptable use. The School cannot be responsible for direct supervision of every user. The School will, however, make every attempt to provide a safe and secure computing and information management system for its users.

The Director and/or his/her designee is responsible for the overall system coordination and relationships with regional, state, national, and/or international network programs.

The Director and/or his/her designee is responsible for instructing and training staff on the acceptable use of the School's computing and networked information systems, maintaining and monitoring the School's computing and information system(s), establishing and maintaining user accounts, and developing and maintaining security and virus protection systems.

The Director and/or designated administrators/supervisors are responsible for ensuring that all staff members receive information about School policies and appropriate instruction and training regarding acceptable use. The Director will also be responsible for ensuring adequate supervision of all users who use School computing and information systems, establishing procedures for conducting building-level activities, maintaining, user contracts, and implementing School policies.

Teachers, within the reasonable scope of instructional responsibilities and/or assigned duties are responsible for instructing students on the proper use of computing and information systems and ensuring that all students understand and follow School usage guidelines and rules. Staff computers are provided for staff use only, student use of any administrative, teacher, or other staff computer is strictly prohibited. Electronic technology used on campus is regarded as the property of the UBCTS, subject to discovery, search, or other investigation methods deemed necessary by the Director and/or appropriate supervisor(s). No expectation of privacy exists in regards to use of school owned property.

Parents are responsible for providing their children with direction regarding restrictions above and beyond those imposed by the School. If the child has access to School/county/state/nation dial-up service from the home as part of the educational program of the School, parents are responsible for the supervision of its use. Student access to computing and information systems is predicated upon completion of a signed User Agreement. Parents are also responsible for reinforcing the provisions of the User Agreement.

Individual users are granted permission to use the School's computing and networked information system(s) only by officials of the School. Individuals who do not have

express written permission to use one or more of the School's computers and who do not sign and return a User Agreement on an annual basis shall not use or attempt to use any School computer or information system. Individuals are responsible for obtaining permission to use the School's computing and information systems and to complete and sign a User Agreement. All individual users are expected to act in a responsible, ethical and legal manner in accordance with School policy, accepted rules of network etiquette, and Federal and state law. Specifically, the following are prohibited:

- (1) Obtaining system privileges to which one is not authorized.
- (2) Deliberately attempting to disrupt the performance of the School's computer system(s) and/or to destroy data by spreading computer viruses or by any other means.
- (3) Use of any School computer or information system to facilitate, advocate, condone or participate in illegal activities.
- (4) Use of any School computer or information system for personal or private commercial or financial gain.
- (5) Use of any School computer or information system to make unauthorized purchases and/or services inconsistent with current School purchasing policies and procedures.
- (6) Use of any School computer or information system for non-school related work during instructional time.
- (7) Use of any School computer or information system for non-school related fund-raising.
- (8) Use of any School computer or information system for political campaigning and/or lobbying.
- (9) Use of inappropriate language on any School computer or information system including, but not limited to, that which is obscene, profane, lewd, vulgar, rude, disrespectful, threatening or Inflammatory as determined by the appropriate supervisor.
- (10) Use of any School computer or information system for hate mail, discriminatory remarks and false or defamatory material about a person or group.
- (11) Displaying or generating images, sounds or messages (on screen, computers or printers) which could create an atmosphere of discomfort, intimidation or harassment to others.
- (12) Violations of privacy including, but not limited to, revealing personal information about others.

- (13) Use of any School computer or information system to disrupt the work of others such as, but not limited to, intentionally obtaining or modifying files, passwords and/or data belonging to other users.
- (14) Unauthorized use of a network address, use of pseudonyms or anonymous use.
- (15) Copyright infringement or plagiarism. Students, staff and other users should assume that all works including, but not limited to Web designs, on the Internet are protected by the copyright laws and, thus, should make every attempt to request permission from the creator of the same to use this work.
- (16) Loading or use of unauthorized, as determined by the Director and/or his/her designee, software, games, programs, files or other electronic media.
- (17) Creating and sending or forwarding electronic chain letters.
- (18) "Spamming" which is sending an annoying, unnecessary and/or unsolicited electronic message.
- (19) Actions which constitute the unauthorized copying, cross-assembling or reverse-compiling of programs and data provided by the School.
- (20) Destruction, modification, abuse or unauthorized removal from the School of any piece of computer hardware, software or network system.
- (21) Wastefully using finite resources; such as, paper, ink and electronic memory resources.
- (22) Posting for unauthorized or inappropriate use personal contact information about themselves or others including, but not limited to, home address, school address, work address, home telephone number, work telephone number, etc.
- (23) Use of any School computer or information system by Non-School personnel. Note: Exceptions will be made for visiting speakers and other school related guests with a signed Acceptable Use Policy Form.
- (24) Use of any Non-School supplied computer or information system on School provided connections to bypass implemented security measures and filtering tools.

### Consequences

Pursuant to the School's Acceptable Electronic Technology Use Policy, the consequences for violating said policy and the guidelines promulgated there under include, but are not limited to the following:

Professional employees who fail to comply with the terms of the Acceptable Electronic Technology Use Policy and the Guidelines set forth above shall be subject to disciplinary action.

Support staff employees who fail to comply with the terms of this Acceptable Electronic Technology Use Policy and the Guidelines set forth above shall be subject to disciplinary action.

Disciplinary action shall be dependant upon the severity and/or frequency of the offense. Such action may result in suspension of user privileges, monetary remuneration for damage or time loss, legal action, temporary suspension without pay and/or termination of employment. All disciplinary action shall be in compliance with due process rights.



**Upper Bucks County Technical School  
Staff Computing and Information Systems User Agreement**

**Staff Member**

Name:.....

Position:.....

As an employee of the Upper Bucks County Technical School, I recognize and understand that, by providing access to the School's computing and networked information systems, the School requires all employees to use such systems in accordance with the Acceptable Use Policy and the Guidelines promulgated thereunder.

I acknowledge that I have received, read and understood the School's Acceptable Use Policy and the Guidelines promulgated thereunder.

Signature:.....

Date:.....