

SCHOOL DISTRICT OF CHELTENHAM TOWNSHIP  
ADMINISTRATIVE REGULATION

**816-A**

**ACCEPTABLE USE POLICY: STUDENT USE OF THE COMPUTERS,  
NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS AND INFORMATION SYSTEMS**

Guidelines for Student Use of Computers and Network Facilities

- All use of the Internet, computers, or other District electronic resources will be in support of educational activities.
- Electronic storage areas will be treated like school lockers. The privacy of electronic mail cannot be guaranteed. Teachers and administrators have the right to retrieve and review files to maintain the integrity of the District network and ensure that individuals are using the system responsibly and in compliance with this Policy and applicable laws.
- Students, staff, parents, and teachers have a responsibility to report breaches of network security.
- Students are responsible for the integrity of their own work. Systems occasionally “crash” and files are occasionally lost. The District can make no guarantees regarding reliability of the technical system.
- The District is excited about the educational opportunities becoming available to its students. The smooth operation of our District’s electronic resources relies upon the responsible conduct of all users.
- All student users are expected to abide by generally accepted rules of computer and network etiquette. For their own safety, students should exercise caution and never reveal the personal addresses or phone numbers of students or staff.

a) General Prohibitions

The following activities are not permitted:

1. Any non-school use of District computers, networks and or resources.
2. Sending or displaying inappropriate material as defined in this Policy.
3. Using obscene or offensive language.
4. Harassing others.
5. Damaging vandalizing, or disabling property, including, but not limited to computer workstations or networks.
6. Violating copyright laws or use of another person’s intellectual property without their permission or proper bibliographic reference. This includes copying of commercial software or copying another student’s intellectual property and representing it as one’s own.
7. Using the network for any illegal activity or to facilitate any illegal activity.
8. Unauthorized access to areas of the Internet or areas of the District’ network.
9. Accessing another individual’s materials, information, or files without permission.
10. Wasting limited resources (such as, but not limited to, printer ink and paper).
11. Employing the network for personal financial or commercial gain.
12. Misrepresenting your identity or impersonating another user.
13. Degrading or disrupting equipment or system performance.
14. Intentionally spreading viruses and other destructive programs.

b) Access Prohibitions

The following activities related to access to the District's systems and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.
2. Acquiring or attempting to acquire passwords of others or giving your password to another. Students will be held responsible for the result of any misuse of a student's user name or password while the user's systems access was left unattended and accessible to others, whether intentional or through negligence.
3. Using or attempting to use computer accounts of others with or without consent and regardless of the purpose.
4. Altering a communication originally received from another person or computer with the intent to deceive.
5. Using or attempting to use District resources to engage in or facilitate any illegal act or criminal activity, including, but not limited to arranging for a drug sale or the purchase of alcohol or being involved in a threat against any person or property.
6. Disabling or circumventing or attempting to disable or circumvent any District security program or device, for example, but not limited to, anti-spy ware, anti-spam software, and virus protection software or procedures.
7. Using a program or device designed to disable or circumvent any District security program or device.
8. Transmitting or attempting to transmit electronic communications anonymously or under an alias unless authorized by the District.

c) Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interference with or disruption or attempted interference or disruption of District 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, offensive material, 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 parasite ware or spy ware designed to steal information, or viruses and worms or other hardware or software designed to damage the District systems or any component of the network, strip or harvest information, or completely take over a person's computer.
2. Altering or attempting to alter files, system security software or the systems without authorization.
3. Unauthorized scanning of District systems for security vulnerabilities.
4. Attempting to alter any District computing or networking components (including, but not limited to file servers, bridges, routers, or hubs).
5. 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.
6. Connecting or attempting to connect unauthorized hardware and devices to the District network.

7. Accessing the District network through cables, routers, or any other equipment located on school property.
8. Loading, downloading, using, or attempting to load, download or use unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files.
9. Intentionally or negligently (a) damaging or destroying the integrity of the District's electronic information (b) damaging or destroying the District's computer hardware or software, (c) disrupting the use of District systems; (d) damaging or destroying the District's systems' networking equipment
10. Failing to comply with requests from appropriate supervisors to discontinue activities that threaten the operation or integrity of the District systems.

Students who use their personal computers, as defined by this policy, must adhere to all provisions of this policy on District premises and property (including but not limited to, buses and other vehicles), at District events, or through connection to District network systems.

#### Sanctions and Other Disciplinary Consequences for Improper Use by Students

Students violating any of the rules will face consequences to be determined by their teacher or principal according to the severity or nature of the infraction. Violations may result in loss of access and, in appropriate cases, may involve a report to law enforcement agencies. Consequences may include:

1. Student may be required to make restitution for network or software/hardware damage.
2. Student may be banned from using telecommunication facilities and/or technological equipment for a specified period of time.
3. Student may fail the marking period and/or the class.
4. Student may face suspension, detention, and expulsion.

#### Student Internet/Intranet Permission Form: Attachment A

Attachment A is the District Student User Agreement. Students will not be permitted access to the District networks and Internet unless a completed and signed form is on file with the District.

Please review with your child and retain this copy of the School District of Cheltenham Township *Acceptable Use of Technology* Policy. Return the sheet, which acknowledges receipt of the School District's *Acceptable Use of Technology* Policy to your child's teacher by (date).

**STUDENT USER AGREEMENT**

I acknowledge that I have received and reviewed the School District of Cheltenham Township *Acceptable Use of Technology* Policy for Students, recognize its importance, and understand this policy governs my use of the District networks and Internet. I have been instructed to read and adhere to the provisions of this policy. Additionally, I understand that if I violate the policy, I am subject to School District discipline and could be subject to Internet Service Provider (ISP), as well as local, state and federal legal recourse. I agree to comply with the School District of Cheltenham Township *Acceptable Use of Technology* Policy for Students.

Student's Signature \_\_\_\_\_

Date: \_\_\_\_\_

I acknowledge that I have received and reviewed the School District of Cheltenham Township *Acceptable Use of Technology* Policy for Students recognize its importance, and understand this policy governs my child's use of the District networks and Internet. I consent to my son/daughter's name, personal information, likeness, and image and/or work product being published on the District's Network and/or website:

Parent's Signature \_\_\_\_\_

Date: \_\_\_\_\_