

**TUSCARORA SCHOOL DISTRICT**  
**ACCEPTABLE USE POLICY**  
**NETWORK/ INTERNET, HARDWARE, AND E-MAIL POLICY**

Network and Internet .....	2
Introduction .....	2
Internet Warning .....	2
Authorized Users.....	2
Hardware Policy .....	3
Electronic Communication Devices Policy .....	4
E-mail Policy .....	5
Fair Use Guidelines for Software and Educational Materials .....	5
Appendix A:.....	7
Glossary of Terms .....	7
Appendix B: .....	9
Acceptable Use Policy Agreement for Computing and Internet Access .....	9

# **NETWORK AND INTERNET**

## **INTRODUCTION**

Tuscarora School District account holders are expected to act in a responsible, ethical and law-abiding manner, in accordance with the missions and purposes of the Tuscarora School District. Please note that all activity must adhere to the laws outlined on the local, state and federal levels. Employees and students will be provided with an educational atmosphere and procedures of control that will assure a suitable learning environment. Every user on the TSD network will act as responsible and productive citizens with respect for civic rights and the role of the individual in a democracy. Using the network is a privilege, not a right, and said privilege may be revoked at any time. It is the purpose of this policy to confirm that the user is aware of their privileges when accessing any services provided by the Tuscarora School District or any digital content accessed while utilizing TSD networks and/or TSD owned devices.

## **INTERNET WARNING**

By providing access to computers and other digital devices, the ability to view material that may not be considered to be of the utmost educational value remains a possibility. The Tuscarora School District views information gathered from the Internet in the same manner as reference materials. Specifically, the district supports resources that will enhance the learning environment with directed guidance from the faculty and staff. However, it is impossible to control all materials on a global network and an industrious user may discover inappropriate information. Within school buildings, student access to and use of digital devices will be under teacher supervision and will be monitored as any other classroom activity. The School District, however, cannot prevent the possibility that some users may access material that is not consistent with the educational mission, goals and policies of the school district. The District has taken every reasonable measure to filter unacceptable Internet sites and e-mail as ordered by The Children's Internet Protection Act (CIPA).

CIPA requires schools to teach online safety to students. The Tuscarora School District educates minors about appropriate online behavior, including cyberbullying awareness and how to safely interact with individuals via social media outlets. Online Internet Safety and Digital Citizenship is taught to students in grades K-12 via TSD faculty.

## **AUTHORIZED USERS**

All authorized users shall adhere to the provisions of this policy as a condition for continued use of the Tuscarora School District network. It is a general policy of the district to promote the use of computers in a manner that is responsible, legal and appropriate. This policy is enacted anytime technology is being used. All non-district devices must be approved by the Technology Coordinator before usage at any building. The successful operation of the network and Internet relies heavily on the proper conduct of the users. If a user violates any of these provisions, their account will be terminated and future access will be denied with no exceptions. Each individual who receives an account will receive information pertaining to the proper use of the network. District administrators will decide what constitutes inappropriate use and their decision is final. The user and/or parent signature on this policy indicates that the user has read the terms and conditions carefully and understands their significance.

Security is a high priority. If you believe there is a violation of the terms and conditions presented in this document, you must notify a member of the technology department immediately. The usage of a district account that is not your own is strictly prohibited. In the event that it is determined you have enabled someone to have unauthorized network access, both your account and the unauthorized user's account will be terminated. Any user identified as a security risk will be denied access.

Vandalism will result in termination of all network and equipment privileges. Vandalism includes but is not limited to the following: damaging computers, computer systems or computer networks; the creation or implementation of computer viruses onto any computer or network device, and debilitating or disabling security provisions on any/all TSD equipment. Users are required to abide by the terms and conditions of the law as stated under the Fair Use Guidelines. We ask you to please respect the privacy of other users' files and intellectual property. Violating copyright, or otherwise using another person's intellectual property without his or her prior approval or proper

citation; using another person's passwords; trespassing in another person's folders, work or files, will result in the loss of network privileges. If physical damages result, the user would be required to pay for any and all damages.

Users are expected to maintain the integrity and functionality of all district resources by reporting any malfunctioning equipment to the Tuscarora Technology Department.

Users are reminded not to:

- Move or modify computer equipment, software, peripherals, or network wiring without proper authorization from the Technology Coordinator
- Attempt to bypass or damage any security device (i.e. firewall, content filter, etc.)
- Share computer accounts and/or passwords
- Use networked resources for non-academic purposes. Non-educational uses of the District's network includes, but is not limited to: games, gambling, junk e-mail, chain letters, jokes, sharing of digital photos and media clips, private business activities, raffles, fundraisers, religious activities or political lobbying. Additionally, the network cannot be used for financial gain or for transaction of any business or commercial activities
- Attempt to bypass the Internet filtering system to gain access to sites that have been blocked
- Violate local, state or federal statutes. Please refer to the Pennsylvania Crimes Code for further information regarding these statutes

## **HARDWARE POLICY**

The purpose of this policy is to establish basic guidelines for the responsible use of TSD computer hardware and peripherals. This is to include all hardware available to authorized users regardless of physical location. Please refer to the Glossary of Terms for definitions.

- District hardware remains unmodified of any hardware upgrades, software updates, and settings to the local machine without proper authorization by the Technology Department
- Distributed technology is required to remain with the assigned user and is not to change possession
- District hardware is to be used for educational and/or professional purposes only
- Users are required to report any maintenance and warranty issues to the Technology Department immediately
- All district devices distributed to users are required to be returned to the Technology Department upon completion of the current school year. Exceptions may be made upon review by the Technology Coordinator. If equipment is not turned in by the appropriate date, the user will be subject to consequences determined by the district administrative staff. Consequences that govern use of textbooks also apply to student laptop computers.
- A signed copy of the individual user agreement for laptops must be received by the Technology Department before any equipment is distributed. Deployment of equipment will be determined by the district administrative staff. Please refer to Appendix B for the user agreement.
- Users are reminded that all equipment issued by the district is the property of the Tuscarora School District and could be removed or restricted at any time.

## **ELECTRONIC COMMUNICATION DEVICES POLICY**

Increased student use of school and personal electronic communication devices (ECDs) has both positive and negative consequences. ECDs facilitate student free speech, and schools have incorporated them in teaching and learning with much success. However, student ECD use on and off campus can be abused in a way that negatively affects students, teachers, and the school environment. This policy is intended to support the benefits of ECD use while curtailing possible abuses.

*Please refer to Appendix A for the definitions of terms relating to ECDs and their policies.*

### **A. Scope of the ECD Policy**

- Acts of cyberbullying and sexting are distracting and potentially terrifying forms of mistreatment that disrupt both a student's ability to learn and a school's ability to educate students in a safe environment.
- The school district, through its school administrators and their designees, has the authority to impose regulations on the possession or use of an ECD while students are on campus, while attending school-sponsored activities or while under the supervision and control of school district personnel.

### **B. School's Authority Over School-Owned ECDs On and Off Campus**

- Cyberbullying through the use of school-owned ECDs can begin both on and off campus. Both types have the potential to instantaneously reach a large number of students/employees and could cause material and/or substantial disruptions in a school environment.
- Violations of conditions of using school-owned ECDs may be subject to disciplinary action by the district.

### **C. School's Authority Over Student-Owned ECDs On Campus**

- School personnel possess the discretion to ban ECDs at any time.
- School personnel may confiscate student-owned ECDs when they have reasonable cause to believe that ECDs have been used to bully or harass other students or employees of the school district, or the use of ECDs will materially and substantially disrupt school activities.

### **D. School's Authority Over Student-Owned ECDs Off Campus**

- School officials may regulate students' off-campus use of student-owned ECDs when they can prove there is a strong possibility that the off-campus activity will result in a material disruption of the school environment or a substantial interference with the rights of others.
- School officials may discipline students for their off-campus use of student owned ECDs when:
  - The student had the knowledge that the off-campus ECD communication and/or its effects would appear on campus, meaning that the on-campus consequences were reasonably foreseeable
  - School officials can demonstrate a causal nexus between the students' off-campus activity and a material disruption of the school environment
  - Evidence exists that the off-campus communication caused a substantial interference with the rights of others, including the right of both students and employees to be free from physical and psychological harm.

## E. Enforcement

- The District may take disciplinary action for misuse of ECDs, consistent with the rule implementing this policy. District security, law enforcement, or both may be contacted when school officials reasonably believe that a student's communication through an ECD constitutes a threat to the safety and welfare of members of the school community.

## **E-MAIL POLICY**

The purpose of this policy is to establish basic guidelines for the responsible use of electronic mail (e-mail) in the Tuscarora School District and establish standard practices. Please refer to the Glossary for definition of terms.

The contents of all e-mail messages are the property of Tuscarora School District. A user has no personal right to privacy when utilizing the district's e-mail system. The District reserves the right to monitor and read any or all messages, without notice to the users. Electronic mail is a District-owned business tool and will be managed through the following rules:

- Users should be aware that e-mail messages can be forwarded or read by unintended recipients. Please use caution while drafting the content of your e-mail messages.
- E-mail messages fall under the classification of Public Records, as defined in A.R.S. 39-121 through A.R.S. 39-121.04.
- E-mail messages must be developed in a professional manner with a positive reflection of the District.
- District administration, for purposes of auditing or investigating potential violations of this e-mail policy, may request access from the Technology Coordinator to user e-mail messages. To ensure the overall integrity of the process, such requests must be in writing and approved by the Superintendent, and must be conducted in a manner which minimizes disruption in the workplace. The following levels of management are authorized to request and receive these detailed records within their respective departments.
  - Superintendent
  - Building Administrators
  - Human Resources Director
  - Business Manager
- Users are responsible for the security of the e-mail accounts that have been entrusted to them. Users must maintain reasonable precautions to safeguard their e-mail accounts from unauthorized entry or use.
- Temporary employees and contractors need to have prior approval from the Superintendent or Technology Coordinator to be given access to District e-mail systems, and must abide by all Tuscarora School District policies and regulations.
- Unacceptable use of e-mail includes, but is not limited to:
  - Mass emailing within the district
  - Running or participating in, a private or non-District related activity
  - Any election or campaign activities
  - Issuing or forwarding advertisements of any commercial nature, except items relating to district business that are approved by the department director.
  - Illegal activities or any violation of civil rights or harassment laws.
  - The creation, storage, or exchange of information in violation of copyright laws.
  - Altering or copying a message or attachment belonging to another user without the permission of the originator.

## **FAIR USE GUIDELINES FOR EDUCATIONAL MATERIALS**

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. Furthermore, the illegal installation of copyrighted software or files for use on the School District's computers is expressly prohibited. This includes but is not limited to all forms of licensed software - shrink-wrap, click wrap, browse wrap, and electronic software downloaded from the Internet.

## APPENDIX A:

### GLOSSARY OF TERMS

**Access to Internet** - A computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network that has access to the Internet.

**Commercial Activity** - A "commercial activity" means either a regular course of commercial conduct or a particular commercial transaction or act. The commercial character of an activity shall be determined by reference to the nature of the course of conduct or particular transaction or act, rather than by reference to its purpose.

**Commercial activities** - Including all fundraising activities being promoted by teachers (in support of their families, friends, etc.) are not appropriate uses of the account. This also includes communications/invitations to business gatherings (i.e. Pampered Chef Home parties).

**Computer** - The term "computer" includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.

**Cyber-Bullying** - Refers to online expression via ECDs that falls into one or more of the definitions of bullying.

- Forms of expression include, but are not limited to, verbal comments, graphic and symbolic communication, and written communication via emailing, instant messaging, and blogging and posting on commercial social networking sites.
- A commercial social networking site means a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or creation of web pages or profiles available to others.

**Electronic Communication Devices (ECDs)** - May be *school-owned* or *student-owned*. Both types may include, but are not limited to, telephones, computers, pagers, cellular telephones, text-messaging devices, and personal data assistance devices.

**Electronic Mail or (E-mail)** - Any transmission or receipt of information, including attachments and imbedded objects, across the District network by electronic means, including but not limited to commercial and electronic mail applications, operating systems, messaging capabilities and Internet mail.

**E-Mail Administrator** - The person(s) responsible for maintaining the organization's electronic mail system and all associated data.

**Formal Communication** - Communication of any kind pertaining to public business, which must be preserved as a public record.

**Harmful to Minors** - Any picture, image, graphic image file, or other visual depiction that—

- taken as a whole and with respect to minors, appeals to a prurient Interest in nudity, sex, or excretion;
- 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 a lewd exhibition of the genitals; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

**Intellectual Property** - Rights and products of the mind or intellect, arising under one or more of the following bodies of law: Trade Secrets, Patents, Trademarks, Trade Dress, Copyrights, and Unfair Competition. This includes any body of work developed by an employee working on District business.

**Interactive White Boards** – Large interactive displays that connect to a computer and projector.

**Minor** – An individual who has not attained the age of 17.

**Product Advertisement** - Considered a commercial activity.

**Public Record** - Any information, minutes, files, accounts or other records which a governmental body is required to maintain and which must be accessible to scrutiny by the public. This includes the files of most legal actions. A court will take "judicial notice" of a public record (including hearsay in the record) introduced as evidence. For example: a recorded deed to show transfer of title or a criminal judgment are both public records.

**Public Record includes**

- A record that is made by a public official in pursuance of a duty, the immediate purpose of which is to disseminate information to the public, or to serve as a memorial of official transactions for public reference.
- A record that is required by law to be kept or necessary to be kept, in the discharge of a duty imposed by law to serve as a memorial and evidence of something written, said, or done.
- A written record of transactions of a public officer in his/her office, which is a convenient and appropriate method of discharging his/her duties, and is kept by him/her as such, whether required by express provisions of law or not.
- Few records in the possession or control of a public officer or body generally will not be "public records." Exceptions are: "work in progress," e.g., a work that is not yet finished, or information that is used solely as a memory aide, e.g., "post-it" notes.

**Routine E-Mail Communications** include:

- Scheduling meetings and conference calls
- Notification of legal and policy issues to be resolved in more formal communication
- Requests for information or directives to complete tasks
- Notification of employees' whereabouts (e.g., vacations, conferences, out-of-office work)
- Requests for formal advice and assistance

**Security Problems** - Conditions that compromise the integrity of the network. Security problems could result from the following activities: sharing passwords, staying logged into the system without locking your account, downloading software, etc.

**Sexting** - Taking, possessing, viewing, sharing, or sending pictures, graphic images, text messages, emails, or other material of a sexually explicit nature on an ECD.

**Vandalism** - Any malicious attempt to harm or destroy data of another user, Internet, or other networks.

**APPENDIX B: ACCEPTABLE USE POLICY AGREEMENT FOR COMPUTING AND INTERNET ACCESS**

Tuscarora School District  
Acceptable Use Policy Agreement for Computing and Internet Access

READ CAREFULLY, COMPLETE, AND RETURN TO THE OFFICE AS SOON AS POSSIBLE. USERS SHOULD SIGN THE "USER" SECTION. FOR STUDENTS, PARENT(S)/GUARDIAN(S) MUST ALSO SIGN THE ACCEPTABLE USE POLICY SECTION BELOW.

**USER**

I will abide by the above Terms and Conditions of the Tuscarora School District Acceptable Use Policy agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or other appropriate legal action may be taken.

**FULL NAME (PLEASE PRINT)**

**GRADE/TEACHER (ELEM. ONLY)**

\_\_\_\_\_

**SIGNATURE:** \_\_\_\_\_ **DATE:** \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

**PARENT OR GUARDIAN – ACCEPTABLE USE POLICY**

As the parent or guardian of this student, I have read the Terms and Conditions of the Tuscarora School District Acceptable Use Policy agreement. I understand that this access is designed for educational purposes and the Tuscarora School District has taken available precautions to eliminate controversial material. I also recognize it is impossible for the Tuscarora School District to restrict access to all controversial materials. I will not hold them responsible for materials acquired on the network. I hereby give permission to issue an account for my child to use computers and the Internet and certify that the information contained on this form is correct.

**PARENT OR GUARDIAN NAME (PLEASE PRINT)**

\_\_\_\_\_

**SIGNATURE:** \_\_\_\_\_ **DATE:** \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_