Tonto Basin Technology Policies and Procedures

The IT Department's intention for publishing Policies and Procedures is to provide clear guidelines and expectations aligned with an established mission of providing users with the best resources possible to educate every student.

The IT Department is committed to protecting Tonto Basin School District's users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and FTP, are the property of Tonto Basin School District. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of Tonto Basin School District.

Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every Tonto Basin School District employee and affiliate is required to meet and exceed the standards set forth by Arizona State Law, Federal Law, the Tonto Basin School Board and administrators. It is the responsibility of every computer user to know these guidelines, and to govern themselves accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of the network-related systems within the Tonto Basin School District. These rules are in place to protect the students, staff, and the Tonto Basin School District. Inappropriate use, improper planning, and disregard of these procedures exposes Tonto Basin School District to risks including compromise of network systems and services, possible damage to the network, and legal issues.

Scope

This policy applies to students, employees, contractors, consultants, temporary employees, authorized guests, and other workers at Tonto Basin School District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Tonto Basin School District including all future purchases.

Acceptable Use Policy

Users should be aware that the data they create on the network remains the property of the Tonto Basin School District. Users should have no expectations of expressed or implied privacy.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Network/Internet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager. Using the Tonto Basin School District network is a privilege. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all school board policies and procedures, Arizona state law, and Federal laws.

The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.

The Tonto Basin School District assumes no responsibility for costs associated with loss or damage to devices not owned by Tonto Basin School District while on the network.

For security and network maintenance purposes, the IT Department may monitor equipment, systems, and network traffic at any time.

The Tonto Basin School District's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Passwords, Accounts, and Antivirus Protection

Users, which includes employees, students, and guests of Tonto Basin School District, will be granted access to the network after they have signed the appropriate Network Usage Agreements forms and forwarded them to designated administrator.

Users must keep passwords secure and should not share their accounts. Authorized users are responsible for the security of their passwords and accounts.

Users shall not leave computers unattended while logged on.

Users of Windows based computer's will be required to change their passwords every 60 days as prompted automatically by Windows Active Directory.

Users needing password resets for various programs must contact the IT Department. This authority may be assigned to a site based employee.

Every attempt will be made to identify the user by positive identification. This method may include sight/voice reconciliation, a predetermined security question, or other questions as determined by the School Administrator.

All computers used by students, employees, or guests that are connected to the Tonto Basin School's network, whether owned by the user or Tonto Basin School District, shall be continually executing virus-scanning software with a current virus database.

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Network Security and Administrator Rights

Administrative passwords for the network, servers, computers, wireless access points, and other electronic devices are to be kept strictly confidential and known only by the IT staff members that need them to perform their duties. Distributing passwords of any kind is strictly forbidden.

Wireless access points will be secured with a security mechanism to be determined by the School Administrator. Any attempt to circumvent and/or distribute ways to circumvent this security mechanism is strictly forbidden.

Users of Tonto Basin School District devices may be granted Administrative Rights to those devices. This access will be given as needed to perform job duties. It is the responsibility of the user to not install or download programs that may affect the performance of the device. This privilege may be revoked. The School Administrator or his/her designee will determine if there is another alternative before granting such rights. To satisfy security and audit purposes, other alternatives will always be used when possible.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

Under no circumstances is an employee, student, or authorized guest of Tonto Basin School District authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Tonto Basin School-owned resources, to include the network and Internet.

Users shall not access, download, store, send, or display text, images, movies, or sounds that contain pornography, obscenity, or language that offends or degrades others. Attempts to circumvent or defeat mechanisms put in place by the Tonto Basin School District staff to manage the network is strictly forbidden.

Users shall not attempt to download and/or install services, electronic file sharing mechanisms, games, software, tools, or any executable file including but not limited to the following file types: .exe, .bat, .cmd, .zip, .msi, and .rar.

The list below is not exhaustive, it does, however, provide a framework for activities which fall into the category of unacceptable use.

Unacceptable Use: System and Network Activities

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Tonto Basin School District;

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Tonto Basin School District or the end user does not have an active license is strictly prohibited;

The exporting of software, technical information, encryption software and/or technology;

The introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home;

Using a Tonto Basin School District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;

Making fraudulent offers of products, items, or services originating from any Tonto Basin School District account;

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:

Accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not

limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

Port scanning or security scanning unless prior notification and approval is received beforehand;

Executing any form of network monitoring unless prior notification and approval is received beforehand;

Circumventing user authentication or security of any host, network or account;

Interfering with or denying service to any user other than the user's host (for example, denial of service attack);

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network/Internet; and

Providing information about, or lists of, Tonto Basin School District's users to parties outside the Tonto Basin School District without prior permission from the Superintendent of Schools.

Unacceptable Use: Email and Communications Activities

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages (shall include forms of harassment via social networks). Students shall not use social network sites including, but not limited to, myspace.com, facebook.com, chat rooms, etc.

Students shall not agree to meet with anyone met online.

Unauthorized use, or forging, of email header information.

Solicitation of email or any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited email originating from within Tonto Basin School District's networks of other internet/network service providers on behalf of, or to advertise, any service hosted by Tonto Basin School District or connected via Tonto Basin School's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

IT Technician Responsibilities

It is the responsibility of the IT Technicians to follow the guidelines and policies of the School Administrator, Tonto Basin School District.

Among their other responsibilities, the IT Technicians should use reasonable efforts to:

Respond to requests for support, information, problem determination and problem resolution.

Become familiar with all applicable Tonto Basin School District IT policies.

Participate in required IT Technicians training and regular meetings as determined by the School Administrator.

Take precautions against theft of or damage to the system components and information.

Comply with terms of all hardware and software licensing agreements applicable to the system.

Treat information about, and information stored by, the network users in an appropriate manner; and

Take precautions protecting the security the network and the security and confidentiality of the information contained therein.

Monitoring

In an effort to maintain network security, integrity, and to reduce the risk of Security Incidents the IT Department, at the discretion of the School Administrator, can and will monitor network activity. These monitoring devices/applications include but are not limited to:

Fire wall logs;
Web filtering logs;
Network traffic monitoring;
Active directory monitoring;
Mail scanner logs;
Database, backup, and usage logs on servers; and
Event logs and histories created in individual machines.

Use of Technology Resources in Instruction

Electronic Information Services User Agreement

Details of the user agreement shall be discussed with each potential user of the electronic information services.
When the signed agreement is returned to the school, the user may be permitted use of EIS resources.

Terms and Conditions of Acceptable Use

Each user must:

1. Use the EIS to support personal educational objectives consistent with the educational goals and objectives of the School District.
2. Agree not to submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
3. Abide by all copyright and trademark laws and regulations.
4. Not reveal home addresses, personal phone numbers or personally identifiable data unless authorized to do so by designated school authorities.
5. Understand that electronic mail or direct electronic communication is not private and may be read and monitored by school employed persons.

   Not use the network in any way that would disrupt the use of the network by others.
6. Not use the EIS for Commercial purposes.
7. Follow the District's code of conduct.
8. Not attempt to harm, modify, add/or destroy software or hardware nor interfere with system security.
9. Understand the inappropriate use may result in cancellation of permission to use the educational information services (EIS) and appropriate disciplinary action up to and including expulsion for students.
10. In addition, acceptable use for District employees is extended to include requirements to:
11. Maintain supervision of students using the EIS.
12. Agree to directly log on and supervise the account activity when allowing others to use District accounts
13. Take responsibility for assigned personal and District accounts, including password protection.
14. Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal and District accounts and files by unauthorized persons.

Personal Responsibility

I will report any misuse of the EIS to the administration or system administrator, as is appropriate.

I understand that many services and products are available for a fee and acknowledge my personal responsibility for any expenses incurred without District authorization.

Network Etiquette

I am expected to abide by the generally acceptable rules of network etiquette. Therefore, I will:

Be polite and use appropriate language. I will not send, or encourage others to send, abusive messages.
Respect privacy. I will not reveal any home address or personal phone numbers or personally identifiable information.

Avoid disruptions. I will not use the network in any way that would disrupt use of the system by others.
Observe the following considerations:

1. Be brief.
2. Strive to use correct spelling and make messages easy to understand.
3. Use short and descriptive titles for articles.
4. Post only to known groups or persons.

Services

The School District specifically denies any responsibility for the accuracy of information. While the District will make an effort to ensure access to proper materials, the user has the ultimate responsibility for how the electronic information service (EIS) is used and bears the risk of reliance on the information obtained.

I have read and agree to abide by the School District policy and regulations on appropriate use of the electronic information system, as incorporated herein by reference.

I understand and will abide by the provisions and conditions indicated. I understand that any violations of the above terms and conditions may result in disciplinary action and the revocation of my use of information services.

Name _____

Signature _____ Date _____
(Student or employee)

School _____Grade (if a student) _____

Note that this agreement applies to both student and employee.

The user agreement of a student who is a minor must also have the signature of a parent or guardian who has read and will uphold this agreement.

Parent or Guardian Cosigner

As the parent or guardian of the above named student, I have read this agreement and understand it. I understand that it is impossible for the School District to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired by use of the electronic information services (EIS). I also agree to report any misuse of the EIS to a School District Administrator. (Misuse may come in many forms but can be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, or other issues described in the agreement.)

I accept full responsibility for supervision if, and when, my child's use of the EIS is not in a school setting. I hereby give my permission to have my child use the electronic information service.

Parent or Guardian Name (print) _____

Signature _____ Date _____