Internet Acceptable Use Policy

Board approved: February 7, 2013

Purpose

The goals of this policy are to outline appropriate and inappropriate use of Tuba City Unified School District's Internet resources, including the use of browsers, electronic mail and instant messaging, file uploads and download, and voice communications. IAUP requires that the use of the resources be in accordance with the following guidelines and support the education, research, and educational goals of the District. Use of these services is subject to the following conditions.

Your Account

Internet access at Tuba City Unified School District is controlled through individual accounts and passwords. Department managers are responsible for defining appropriate Internet access levels for the people in their department and conveying that information to the Technology Dept.

Each user (Certified, Classified, Students and Guests) of Tuba City Unified School District's system is required to read this Internet policy and sign an Internet use agreement prior to receiving Internet access/User ID/Login account and password.

Appropriate Use

Individuals at Tuba City Unified School District are encouraged to use the Internet to further the goals and objectives of Tuba City Unified School District. The types of activities that are encouraged include:

1. Communicating with fellow employees, business partners of Tuba City Unified School District and clients within the context of an individual's assigned responsibilities;
2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
3. Participating in educational or professional development activities.

Inappropriate Use

Individual Internet/User ID/Login use will not interfere with others' productive use of Internet resources. Users will not violate the network policies of any network accessed through their account. Internet use at Tuba City Unified School District will comply with all Federal and State laws, all Tuba City Unified School District policies, and all Tuba City Unified School District contracts. This includes, but is not limited to, the following:

1. The Internet/User ID/Login may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
2. The Internet/User ID/Login may not be used in any way that violates Tuba City Unified School District's policies, rules, or administrative orders including, but not limited to, Board Approved policies. Use of the Internet in a manner that is not consistent with the mission of Tuba City Unified School District, misrepresents Tuba City Unified School District, or violates any Tuba City Unified School District policy is prohibited.
3. Individuals should limit their personal use of the Internet unless otherwise. Tuba City Unified School District allows limited personal use for communication with family and friends, independent learning, and public service unless otherwise. Tuba City Unified School District prohibits use for mass unsolicited mailings, access for non-employees to Tuba City Unified School District resources or network facilities, uploading and downloading of files for personal use, access to restricted sites, gaming, competitive commercial activity unless pre-approved by Tuba City Unified School District and the dissemination of chain letters.
4. Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by management.
5. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Tuba City Unified School District or another individual without authorized permission.
6. In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business/classroom purposes.
7. Individuals will only use Tuba City Unified School District approved services, specifically PR, Interviews and School Related functions for voice communication over the Internet.

District Issued Equipment

Teachers, Staff and Students of Tuba City Unified School District that have District issued technology equipment (Laptops, Tablets, Workstations, Printers etc.,) must return them to the Technology Department or Supervisor to receive their final payout (teachers only) or upon resignation or termination.

Any District issued technology equipment (laptops and tablets) that are damaged, lost or stolen by the District employee or student due to misuse and negligence is subject to pay for any District owed property upon review by their Supervisor/Principal and Technology Director.

Security

For security purposes, users may not share account or password information with another person. Internet/User ID/Login accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the Technology Department to obtain a password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to Internet services.

Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at Tuba City Unified School District. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of the Internet may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
2. Disciplinary action according to applicable Tuba City Unified School District policies.
3. Legal action according to applicable laws and contractual agreements.

Monitoring, Filtering and Internet Safety

Tuba City Unified School District's Technology Department may monitor any Internet activity occurring on Tuba City Unified School District's equipment or accounts. Tuba City Unified School District currently does employ filtering software (Barracuda Content Filter) to limit access to sites on the Internet. If Tuba City Unified School District discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

Tuba City Unified School District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. Tuba City Unified School District is not responsible for any service interruptions, changes, or consequences. Tuba City Unified School District reserves the right to establish rules and regulations as necessary for the efficient operation of the Internet Acceptable Use Policy.

Tuba City Unified School District does not assume liability for any information lost, damaged, or unavailable due to technical or other difficulties.

As required by the Children's Internet Protection Act, Tuba City Unified School District shall provide for technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or with respect to use of the computers by students, harmful to students. The protective measures shall also include monitoring the online activities of students and staff.

Limits, controls, and prohibitions shall be placed on the student and staff:

- access to inappropriate matter and content.
- safety and security in direct electronic communications.
- unauthorized online access or activities.
- unauthorized disclosure, use and dissemination of personal information.

Education, Supervision and Monitoring

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies and administrative guidelines and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment 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, and the Protecting Children in the 21st Century Act.

The Technology Department shall provide for appropriate training for District employees and for the students who use the District's computer network and have access to the Internet, Training provided shall be designated to promote the District's commitment to:

- the standards and acceptable use of the District's network and Internet services as set forth in District policy.
- student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social networking websites, online opportunities and chat rooms; and cyber-bullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of the policy and the accompanying regulation, regardless of whether training has been given.

The Technology Director is responsible for the implementation of this policy and for establishing and enforcing the District's Internet Acceptable Use Policy guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

Disclaimer

Tuba City Unified School District assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. Tuba City Unified School District is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

We encourage you to use your Internet/User ID/Login access responsibly. Should you have any questions regarding this Internet Acceptable Use Policy, feel free to contact the Technology Department at techsupport@tcusd.org or the Technology Director.

Internet Acceptable Use Policy User Agreement

I hereby acknowledge that I have read and understand the Internet Acceptable Use Policy of Tuba City Unified School District. I agree to abide by these policies and ensure that persons working under my supervision and students abide by these policies. I understand that if I violate such rules, I may face legal or disciplinary action according to applicable law or departmental policy.

I hereby agree to indemnify and hold Tuba City Unified School District and its officers, trustees, employees, and agents harmless for any loss, damage, expense or liability resulting from any claim, action or demand arising out of or related to the user's use of Tuba City Unified School District owned computer resources and the network, including reasonable attorney fees. Such claims shall include, without limitation, those based on trademark or service mark infringement, trade name infringement, copyright infringement, unfair competition, defamation, unlawful.

Password Policy

Purpose

Passwords are an important component of information and network security. The use of a User ID/Login and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to provide the guidelines necessary for all of the employees of Tuba City Unified School District to create appropriate passwords and to use them and protect them in an appropriate manner.

Scope

This policy applies to all employees of Tuba City Unified School District who have any form of computer or application account that requires password access. Examples of accounts include:

- Workstation (desktop/laptop/tablet)
- Network
- E-mail system
- Accounting application (Infinite Visions Enterprise, Quickbooks, etc.)
- Customer information database (SchoolDude, RTA)

Please note: This list is not intended to be all-inclusive; it is simply provided for reference purposes.

Policy

General

1. Password construction, lifecycle and re-use parameters will be variable according to the classification of the system or data that they are intended to protect.
2. Passwords should not be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary.
3. Users will be notified one week in advance of password expiration. At that point, and at every subsequent login until a change is made, users will be prompted to select a new password.
4. Tuba City Unified School District will use technical measures to ensure that users conform to the policy.
5. All passwords must conform to the guidelines outlined below.

Password Construction Guidelines

1. Passwords used to access data classified as "Secret" or the systems that host this data (Servers, Routers, Firewalls, Switches) must be a minimum of ten (10) characters in length. Further, these

passwords must use at least one character of the four-character types, those being lower case letters, upper case letters, numbers and special characters. Applies to Technology Dept.

2. Passwords used to access data classified as "Confidential" or the systems that host this data (Accounting Software eg: Infinite Visions Enterprise, Quickbooks) must be a minimum of eight (8) characters is length. Further, these passwords must use at least one character of three of the four-character types, those being lower case letters, upper case letters, numbers and special characters. Applies to District Office Users or Users with Access to Infinite Visions Enterprise.

3. Passwords used to access data classified as "Private" or the systems that host this data (Standard Workstations/Laptops and District Labs) must be a minimum of six (8) characters in length. Further, these passwords must use at least one character of two of the four-character types, those being lower case letters, upper case letters, numbers and special characters. Applies to Teachers, Students, Non-Specific Classified Employees and Guest Users.

4. Passwords are not needed to access data classified as "Public" or the systems that host this data, as long as these systems do not host data of a higher classification level and so no construction guidelines need to be set.

Password Lifecycle Guidelines

1. Passwords used to access data classified as "Secret" or the systems that host this data will have a maximum age of one (1) month and a minimum age of one (1) month. As such, passwords must be changed every month and cannot be changed more frequently. Where the application or system can only be specified to change on the basis of a variable number of days, maximum and minimum age will be set at thirty (30) days.

2. Passwords used to access data classified as "Confidential" or the systems that host this data will have a maximum age of three (3) months and a minimum age of two (2) weeks. As such, passwords must be changed every three (3) months and cannot be changed more frequently than every two (2) weeks. Where the application or system can only be specified to change on the basis of a variable number of days, maximum age will be set at ninety (90) days and minimum age at fourteen (14) days.

3. Passwords used to access data classified as "Private" or the systems that host this data will have a maximum age of six (6) months and a minimum age of one (1) week. As such, passwords must be changed every six (6) months and cannot be changed more frequently than everyone (1) week. Where the application or system can only be specified to change on the basis of a variable number of days, maximum age will be set at one hundred and eighty (180) days and minimum age at seven (7) days. For Students there is set standard for passwords and all student user ID/logins have restricted access.

4. Passwords are not needed to access data classified as "Public" or the systems that host this data, as long as these systems do not host data of a higher classification level and so no lifecycle guidelines need to be set.

Password Reuse Guidelines

1. Passwords used to access data classified as "Secret" or the systems that host this data may never be reused once they have expired. As such a completely new password is required at each expiry. "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

2. Passwords used to access data classified as "Confidential" or the systems that host this data may be reused every sixth password. As such a completely new password is required for the first five expiries; thereafter the first password can be reused. "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

3. Passwords used to access data classified as "Private" or the systems that host this data may be reused every third password. As such a completely new password is required for the first two expiries; thereafter the first password can be reused. "Completely new" is defined as having at least fifty percent (50%) of the characters different from the previous password.

4. Passwords are not needed to access data classified as "Public" or the systems that host this data, as long as these systems do not host data of a higher classification level and so no reuse guidelines need to be set.

Password Protection Guidelines

1. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members.

2. Under no circumstances will any member of the organization request a password without the request coming from both a representative of the IT department and the user's direct manager. Should a request be made that does not conform to this standard, immediately inform both the IT department and your direct manager.

3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company's Virtual Private Network or SSL-protected Web site.

4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

5. Do not use the "Remember Password" feature of applications.

6. Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work related accounts are not to be used to access company accounts.

7. Each application, system and data point should be protected by a different password where possible. The use of the same password to protect all access is strongly discouraged.

8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately. If the minimum aging requirement has not been met for the password, the IT department will reset the minimum aging for the account allowing the user to create a new password.

9. The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action.