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 and students 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 and students 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.

Tuba City Unified School District #15

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 (6) 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 every one (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 or student 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.

Tuba City Unified School District #15

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 or student who is found to have violated this policy may be subject to disciplinary action.

Password Policy User Agreement

I hereby agree to the terms and conditions of Tuba City Unified School District’s Password Policy.

_____
Employee/Student Name (print)

_____ _____
Employee Signature/Student Date

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.

Public Awareness Notification

➢ Child Find

Schools are required to locate, identify and evaluate **all children** with disabilities from **birth through age 21**. The Child Find mandate applies to all children who reside within a State, including children who attend private schools and public schools, highly mobile children, migrant children, homeless children, and children who are wards of the state.

This includes all children who are suspected of having a disability, including children who receive passing grades and are "**advancing from grade to grade**."

➢ Availability of Special Education and Related Services

The Tuba City Unified School District #15 works collaboratively with the Tribal Agencies to locate special needs students who may qualify for special education and related services. The TCUSD#15 child find efforts include:

- Referrals of all preschool children ages 2.9 years through 5 years of age to the school district of parent residence.
- Referrals of all school age children ages 5 years through 21 years of age to the school district of the parent's residence.

- For additional information concerning pre-school or school age students please contact the district, in which the student resides, or contact:
  - ☎ Sandra Roe, Exceptional Student Services Supervisor
  - ☎ Rhonda Chase, ESS Data Specialist
    928-283-1160
    PO Box 67
    Tuba City, AZ 86045
- **New and transfer students**
  - The district routinely reviews records of newly enrolled students for information about prior screenings, evaluations and progress in schools.
  - The district routinely screens all new kindergarten students and those newly enrolled students within 45 calendar days.

➢ Policies and Procedures

The Governing Board approved policies and procedures for Special Education Students are available at the individual school sites, and also available for review at the Exceptional Student Services Department. Please contact 928-283-1160 to obtain a set of policies and procedures. They will be mailed out upon request, at no cost to parents and community members.

➢ Procedural Safeguards

TCUSD#15 ensures that children with disabilities and their parents are guaranteed procedural safeguards with respect to the provision of Free and Appropriate Public Education (FAPE). Procedural safeguards are provided to the parents annually and upon request.

Annual Notification to Parents Regarding Confidentiality of Student Education Records

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school within 45 days of a request made to the school administrator. Schools are not required to provide copies of records unless it is impossible for parents or eligible students to review the records without copies. Schools may charge a fee for copies.
- Parents or eligible students have the right to request in writing that a school correct records that they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:
  - School officials with legitimate educational interest
    - A school official is a person employed or contracted by the school to serve as an administrator, supervisor, teacher, or support staff member (including health staff, law enforcement personnel, attorney, auditor, or other similar roles); a person serving on the school board; or a parent or student serving on an official committee or assisting another school official in performing his or her tasks;
    - A legitimate educational interest means the review of records is necessary to fulfill a professional responsibility for the school;
  - Other schools to which a student is seeking to enroll;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, sports participation (including height and weight of athletes) and dates of attendance unless notified by the parents or eligible student that the school is not to disclose the information without consent.

The Individuals with Disabilities Education Act (IDEA) is a federal law that protects the rights of students with disabilities. In addition to standard school records, for children with disabilities education records could include evaluation and testing materials, medical and health information, Individualized Education Programs and related notices and consents, progress reports, materials related to disciplinary actions, and mediation agreements. Such information is gathered from a number of sources, including the student's parents and staff of the school of attendance. Also, with parental permission, information may be gathered from additional pertinent sources, such as doctors and other health care providers. This information is collected to assure the child is identified, evaluated, and provided a Free Appropriate Public Education in accordance with state and federal special education laws.

Each agency participating under Part B of IDEA must assure that at all stages of gathering, storing, retaining and disclosing education records to third parties that it complies with the federal confidentiality laws. In addition, the destruction of any education records of a child with a disability must be in accordance with IDEA regulatory requirements.

For additional information or to file a complaint, you may call the federal government at (202) 260-3887 (voice) or 1-800-877-8339 (TDD) OR the Arizona Department of Education (ADE/ESS) at (602) 542-4013. Or you may contact:

Family Policy Compliance Office U.S. Department of Education 400 Maryland Avenue, SW Washington, D.C. 20202-5901	Arizona Department of Education Exceptional Student Services 1535 W. Jefferson, BIN 24 Phoenix, AZ 85007

This notice is available in English and Spanish on the ADE website at www.ade.az.gov/ess/resources under forms. For assistance in obtaining this notice in other languages, contact the ADE/ESS at the above phone/address.

Tuba City Unified School District No. 15

COVID-19 Protocols
What You Need to Know

INTRODUCTION

The following are key elements of the COVID-19 mitigation strategies for welcoming students back to in-person learning. For more information, please refer to the COVID-19 Protocol documents available any time on the District website. You may also contact your school site principal or the District office at 928-283-1001.

STAY HOME IF YOU DON'T FEEL WELL

Anyone who feels sick should not enter a TCUSD school site or facility.

ENTERING SCHOOL SITES

Students and other visitors entering a school site will be subject to daily health screening questions and temperate checks. Only essential groups are allowed in school sites and facilities, including students and staff.
Parents/guardians will only be allowed on-site with confirmed appointment and/or approval of site administrator.

FACE COVERINGS ARE REQUIRED AT ALL TIMES

All persons are required to correctly wear a face covering at all times in TCUSD school sites and facilities.

KEEP YOUR DISTANCE

All persons are required to maintain a minimum six (6) feet distance between themselves and others at all times.

HANDWASHING

All persons are required to wash their hands regularly throughout the day.
Hand sanitizer is readily available in all TCUSD settings to supplement handwashing

CLEANING & DISINFECTING

Custodial staff will utilize disinfectant "fogger" machines to regularly disinfect classrooms.
Teaching and support staff will supplement these efforts by periodically cleaning/disinfecting their classrooms.
Cleaning/disinfecting will not take place when students or other staff are in the environment.
Students will not be asked to assist in cleaning/disinfecting efforts.

ENVIRONMENTAL & OPERATIONAL ALTERATIONS

Alterations to school sites to promote the mitigation strategies include adjustments to hallway flow of foot traffic, rearranging of desks in classrooms and/or the provision of physical barriers where necessary, restroom usage and communal drinking fountain adjustments, closure of playground equipment and cafeteria setting for meal delivery (where feasible) with alternative strategies for physical activity and meal delivery established.

TCUSD is administering these efforts to mitigate, or reduce the likelihood of the spread of COVID-19.
Please understand these efforts cannot completely eliminate concerns related to the COVID-19 pandemic.
The COVID-19 pandemic is constantly changing. As such, TCUSD may revise these strategies as necessary.

Arizona COVID-19 Guidance
'Release from Quarantine & Isolation' Flow Chart

Has the patient tested POSITIVE for COVID-19?

YES

ISOLATE for 5 DAYS

SYMPTOMS

Symptoms NOT resolving after 5 days

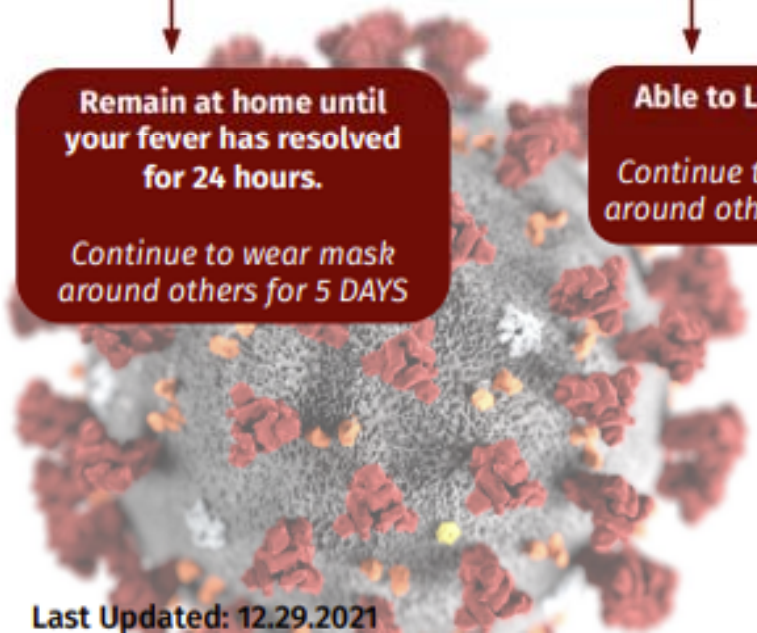
Remain at home until your fever has resolved for 24 hours.

Continue to wear mask around others for 5 DAYS

Symptoms resolving after 5 days

NO SYMPTOMS

Able to LEAVE house
&
Continue to wear mask around others for 5 DAYS



Has the patient been EXPOSED to someone who tested POSITIVE for COVID-19?

YES

FULLY VACCINATED*

OR

PARTIALLY VACCINATED or NOT VACCINATED**

NO QUARANTINE

- **WEAR A MASK** around others for 10 days
- **TEST** on day 5, if possible

If you develop symptoms, get tested and stay home.

QUARANTINE

- **Stay home for 5 days & wear a mask around others for 5 additional days**
- **TEST** on day 5, if possible

If you develop symptoms get a test and stay home.

If you CANNOT quarantine you must wear a mask for 10 days.

**Fully vaccinated: Completion of a 2-dose series within 6 months; OR completion of a single-dose series within 2 months; OR completion of primary series AND received a booster dose.*

***Partially vaccinated: Primary series not completed; OR primary series completed, but NOT boostered (2 months after 1-dose series, 6 months after 2-dose series).*

Last Updated: 12.29.2021

ARIZONA GUIDE TO IMMUNIZATIONS REQUIRED FOR ENTRY

Grades K-12 (School year 2021-2022)

- Requirements are shown below as stated in Arizona Administrative Code, R9-6-702, Table 7.1 and Table 7.2
- Please review the Arizona Immunization Handbook for Schools and Child Care Programs along with the Vaccine Catch-up Flowcharts & FAQs for further information and details about immunization requirements and exemptions.
- Vaccines must follow ACIP minimum intervals and ages to be valid. See page 2 for minimum interval and catch-up schedule information.
- The 4-day grace period only applies to vaccine-administration minimum age and intervals. Refer to the Handbook for questions.

Vaccine	4-6 Years Old and attendance in Kindergarten or 1st grade	7-10 Years Old	11 Years and Older
HepB Hepatitis B	**3 doses** The final dose of HepB must be given at 24 weeks of age or older. Only 3 doses are required if the 3rd dose was received at or after the child was 24 weeks of age; otherwise 4 doses are required.		
Polio Poliomyelitis (IPV) For OPV see page 2	**4 doses** The final dose of polio must be received at/after 4 years of age and at least six months after the previous dose. Only 3 doses are required if the 3rd dose was received on/after the child's 4th birthday and at least six months after the 2nd dose. Additional doses may be needed to meet requirements. See pg. 2 for retrospective history guidance.		
MMR Measles, Mumps and Rubella	**2 doses** Minimum recommended age for dose 1 is 12 months. A 3rd dose will be required if dose 1 was given more than 4 days before 1st birthday.		
VAR Varicella (chickenpox)	**1 dose** Minimum recommended age for dose 1 is 12 months. 2 doses, at least 4 weeks apart, are required if dose 1 was given at 13 years of age or older.		
DTaP, Tdap, Td Diphtheria, Tetanus, and Pertussis	**5 doses of DTaP** The final dose of tetanus-diphtheria containing vaccine must be received at/after 4 years of age and at least six months after the previous dose. Only 4 doses are required if the 4th dose was received on/after 4 years of age; in certain situations an additional dose may be required, up to a maximum of 6 doses (before age 7).	**4 doses of tetanus-diphtheria-containing vaccine (or combination of DTaP, Td or Tdap doses). At least one dose at/after 4 years of age and at least 6 months from previous dose.** 3 doses (with one at/after 4 years) is acceptable if the first dose was given on/after 1st birthday; otherwise refer for an additional dose.	**1 dose of Tdap is required** If the student does not have a Tdap but received a dose of tetanus-diphtheria-containing vaccine within the past 5 years, refer for the adolescent Tdap dose when 5 years has passed since that dose. If a student has received 1 valid dose of adolescent Tdap (age 10 years or older), no further doses are needed. Students must have minimum series of 4 doses of tetanus-diphtheria-containing vaccine; 3 doses acceptable if the 1st dose was given on/after 1st birthday.
MenACWY or MCV4 Quadrivalent Meningococcal	Retrospectively: Menomune (Meningococcal Polysaccharide) vaccine was a quadrivalent vaccine so is acceptable; however, production of this vaccine was discontinued in February 2017. Menomune doses are considered acceptable for school requirements.		**1 dose of MenACWY is required** A dose administered at 10 years of age will meet the requirement.

ARIZONA GUIDE TO IMMUNIZATIONS REQUIRED FOR ENTRY – Minimum Interval/Catch-up Guidance

Grades K-12 (School year 2021-2022)

Vaccine	Dose #	Minimum Age	Minimum Interval Between Doses	Notes
HepB Hepatitis B	dose 1	Birth	At least 4 weeks between dose 1 & 2	• Some children may receive a birth dose and then a combination vaccine resulting in a total of 4 (or more) doses. At long as the interval between doses is met, 4+ doses meet requirement. • 2 doses, at least 4 months apart, meet the requirement if the child received the adolescent series using the Merck Recombivax HB Adult Formulation when the child was 11-15 years of age.
	dose 2	4 weeks	At least 8 weeks between dose 2 & 3 (or final)	
	dose 3	24 weeks	At least 16 weeks between dose 1 & 3 (or final) AND at/after 24 weeks of age	
Polio IPV or OPV	dose 1	6 weeks	At least 4 weeks between dose 1 & 2	• Retrospectively: 1) A final dose given on or after August 7, 2009, must be given at or after 4 years of age **and** a minimum interval of 6 months from the previous dose. 2) Students who received 4 doses (with at least 4 weeks minimum intervals between doses and/or before the age of 4 years) PRIOR to August 7, 2009 have met the requirement. • OPV given prior to April 1, 2016 will be presumed to be trivalent and therefore acceptable, regardless of age, or country, of administration. Any OPV doses administered on or after April 1, 2016 are presumed to be bivalent and therefore unacceptable. • Poliomyelitis vaccine is not recommended in the U.S. for individuals 18 years of age or older; however, a complete series is still required for school attendance.
	dose 2	10 weeks	At least 4 weeks between dose 2 & 3	
	dose 3	14 weeks	At least 4 weeks between dose 3 & 4	
	dose 4	4 years	At least 6 months between final dose and previous dose (could be final dose 3 or final dose 4)	
MMR Measles, Mumps and Rubella	dose 1	12 months	At least 4 weeks (28 days) between dose 1 & 2	• If MMR dose 1 was given more than 4 days before the 1st birthday, another dose is required. • MMR and varicella vaccines are live vaccines and must be given on the same day or at least 28 days apart (this rule also applies to live nasal influenza doses).
	dose 2	13 months	-	
VAR Varicella (chickenpox)	dose 1	12 months	At least 3 months between dose 1 & 2 4 weeks (28 days) between doses if administered at age 13 or older	• If varicella dose 1 was given more than 4 days before the 1st birthday, another dose is required. • MMR and varicella vaccines are live vaccines and must be given on the same day or at least 28 days apart (this rule also applies to live nasal influenza doses).
DTaP, Tdap, Td Tetanus, Diphtheria, and Pertussis	dose 1	6 weeks	At least 4 weeks between dose 1 & 2	• DTaP is licensed for children through age 6. If catch-up doses are needed at age 7 or older, Tdap or Td should be used to start/complete the series. • A Tdap given at age 7-9 years of age does not count for the 11- year old Tdap requirement; a Tdap should be given once 5 years has passed since last dose of tetanus-diphtheria containing vaccines was given. • Retrospectively, if a child received a Tdap at age 10 as part of a catch-up series, or inadvertently earlier than the recommended age of 11-12, the dose may be counted as the adolescent dose and is acceptable to meet school requirements. • Once a valid adolescent Tdap dose has been received, a tetanus booster is recommended when 10 years has passed since last dose of tetanus-containing vaccine.
	dose 2	10 weeks	At least 4 weeks between dose 2 & 3	
	dose 3	14 weeks	At least 6 months between dose 3 & 4	
	dose 4	12 months	At least 6 months between dose 4 & 5	
	dose 5	4 years	In general, a child should not receive more than 4 doses prior to the 4th birthday or a total of 6 doses prior to the 7th birthday; however, the child should still receive a dose at/after 4 years of age and at least 6 months from previous dose	
MenACWY, MCV4 Meningococcal	dose 1	10 years		• Only quadrivalent meningococcal ACWY vaccine doses will be accepted. The vaccines given currently in the U.S. are Menactra, Menveo, and MenQuadfi. No monovalent or bivalent meningococcal vaccinations will be accepted (MenA, MenB, MenC, or MenC/Y).

Arizona Immunization Program Office • 150 North 18th Avenue, Suite 120
Phoenix, AZ 85007 • (602) 364-3630
Last reviewed/revised June 2021

VACCINE INFORMATION STATEMENT

Meningococcal B Vaccine:

What You Need to Know

Many Vaccine Information Statements are available in Spanish and other languages. See www.immunize.org/vis

Hojas de información sobre vacunas están disponibles en español y en muchos otros idiomas. Visite www.immunize.org/vis

1 Why get vaccinated?

Meningococcal B vaccine can help protect against **meningococcal disease** caused by serogroup B. A different meningococcal vaccine is available that can help protect against serogroups A, C, W, and Y.

Meningococcal disease can cause meningitis (infection of the lining of the brain and spinal cord) and infections of the blood. Even when it is treated, meningococcal disease kills 10 to 15 infected people out of 100. And of those who survive, about 10 to 20 out of every 100 will suffer disabilities such as hearing loss, brain damage, kidney damage, loss of limbs, nervous system problems, or severe scars from skin grafts.

Anyone can get meningococcal disease but certain people are at increased risk, including:

- Infants younger than one year old
- Adolescents and young adults 16 through 23 years old
- People with certain medical conditions that affect the immune system
- Microbiologists who routinely work with isolates of *N. meningitidis*, the bacteria that cause meningococcal disease
- People at risk because of an outbreak in their community

2 Meningococcal B vaccine

For best protection, more than 1 dose of a meningococcal B vaccine is needed. There are two meningococcal B vaccines available. The same vaccine must be used for all doses.

Meningococcal B vaccines are recommended for people 10 years or older who are at increased risk for serogroup B meningococcal disease, including:

- People at risk because of a serogroup B meningococcal disease outbreak
- Anyone whose spleen is damaged or has been removed, including people with sickle cell disease
- Anyone with a rare immune system condition called "persistent complement component deficiency"
- Anyone taking a type of drug called a complement inhibitor, such as eculizumab (also called Soliris®) or ravulizumab (also called Ultomiris®)
- Microbiologists who routinely work with isolates of *N. meningitidis*

These vaccines may also be given to anyone 16 through 23 years old to provide short-term protection against most strains of serogroup B meningococcal disease; 16 through 18 years are the preferred ages for vaccination.

3 Talk with your health care provider

Tell your vaccine provider if the person getting the vaccine:

- Has had an **allergic reaction after a previous dose of meningococcal B vaccine**, or has any **severe, life-threatening allergies**.
- Is **pregnant or breastfeeding**.

In some cases, your health care provider may decide to postpone meningococcal B vaccination to a future visit.

People with minor illnesses, such as a cold, may be vaccinated. People who are moderately or severely ill should usually wait until they recover before getting meningococcal B vaccine.

Your health care provider can give you more information.

U.S. Department of Health and Human Services
Centers for Disease Control and Prevention

4 Risks of a vaccine reaction

- Soreness, redness, or swelling where the shot is given, tiredness, fatigue, headache, muscle or joint pain, fever, chills, nausea, or diarrhea can happen after meningococcal B vaccine. Some of these reactions occur in more than half of the people who receive the vaccine.

People sometimes faint after medical procedures, including vaccination. Tell your provider if you feel dizzy or have vision changes or ringing in the ears.

As with any medicine, there is a very remote chance of a vaccine causing a severe allergic reaction, other serious injury, or death.

5 What if there is a serious problem?

An allergic reaction could occur after the vaccinated person leaves the clinic. If you see signs of a severe allergic reaction (hives, swelling of the face and throat, difficulty breathing, a fast heartbeat, dizziness, or weakness), call **9-1-1** and get the person to the nearest hospital.

For other signs that concern you, call your health care provider.

Adverse reactions should be reported to the Vaccine Adverse Event Reporting System (VAERS). Your health care provider will usually file this report, or you can do it yourself. Visit the VAERS website at **www.vaers.hhs.gov** or call **1-800-822-7967**. *VAERS is only for reporting reactions, and VAERS staff do not give medical advice.*

6 The National Vaccine Injury Compensation Program

The National Vaccine Injury Compensation Program (VICP) is a federal program that was created to compensate people who may have been injured by certain vaccines. Visit the VICP website at **www.hrsa.gov/vaccinecompensation** or call **1-800-338-2382** to learn about the program and about filing a claim. There is a time limit to file a claim for compensation.

7 How can I learn more?

- Ask your healthcare provider.
- Call your local or state health department.
- Contact the Centers for Disease Control and Prevention (CDC):
  - Call **1-800-232-4636** (**1-800-CDC-INFO**) or
  - Visit CDC's **www.cdc.gov/vaccines**

Vaccine Information Statement (Interim)
Meningococcal B Vaccine

Office use only

8/15/2019 | 42 U.S.C. § 300aa-26

Arizona Department of Education
Arizona Residency Guidelines
REVISED 11/08/2021

Disclaimer: The Arizona Department of Education is providing these guidelines as technical assistance to the field. These guidelines are how the Arizona Department of Education interprets the below statutes and are not binding nor is it legal advice. If you have any legal questions, please consult an attorney.

INTRODUCTION

Local educational agencies are required to provide all children who reside within the school district with equal access to public education at the elementary and secondary level. The U.S. Supreme Court held in *Plyer v. Doe*, 457 U.S. 202 (1982), that the undocumented or non-citizen status of a student (or his or her parent/guardian) is irrelevant to that student's entitlement to an elementary and secondary public education. However, pursuant to A.R.S. § 15-823, a school district or charter school may not include non-Arizona-resident pupils in their student count and may not obtain state aid for those pupils.

In Arizona, the "district of residence" of a student is determined by the residency of the parent or guardian with whom the student lives. In some cases, the district of residence may also be determined by the residency of a relative who is seeking legal guardianship or custody of a student. A.R.S. § 15-821(D). In addition, if a school district governing board determines that a student's "physical, mental, moral or emotional health is best served by placement with a grandparent, brother, sister, stepbrother, stepsister, aunt or uncle who is a resident within the school district," and the placement with that relative is not "solely for the purpose of obtaining an education in this state without payment of tuition," the student is considered a resident of the district. A.R.S. § 15-823(C).[1]

Accordingly, it is the responsibility of the school districts and charter schools that receive state aid to ensure that student/parent residency information is accurate and verifiable. **While a district may restrict attendance to district residents based on available classroom space,[2] inquiring into students' citizenship or immigration status, or that of their parents or guardians, is not relevant to establishing residency within the district. A school district or charter school may not bar a student from enrolling because he or she lacks a birth certificate or has records indicating a foreign place of birth, such as a foreign birth certificate.[3]**

The Arizona Department of Education may audit schools to ensure that only Arizona resident students are reported for state aid. Any school district or charter school that cannot demonstrate the accuracy of any student's residency through documents provided by the parent/guardian may be required to repay the state aid received for that student. The following are examples of verifiable documentation parents may provide to demonstrate that they reside in a district.

[1] *See also Martinez v. Bynum*, 461 U.S. 321 (1983).
[2] Pursuant to A.R.S. § 15-816 and A.R.S. § 15-816.01, Arizona's mandatory open enrollment policies allow a student to apply for admission and transfer to any public school of his or her choice, based on available classroom space, even if it is outside of the student's district of residence. There are two basic types of open enrollment policies: 1) Intra-district: Students transfer to another school within the resident school district, or 2) Inter-district: Students transfer to a school outside of their resident district.
[3] For more information, please read https://www2.ed.gov/about/offices/list/ocr/letters/colleague-201405.pdf.

VERIFIABLE DOCUMENTATION

A.R.S. § 15-802(B) requires school districts and charter schools to obtain and maintain verifiable documentation of Arizona residency upon enrollment in an Arizona public school. This document is designed to assist school districts and charter schools in meeting the legal requirements of the statute.

The documentation required by A.R.S. § 15-802 **must be provided at initial enrollment of a student in a school district or charter school in this state and reaffirmed, although not necessarily recollected, during the district or charter's annual registration process. This process will vary by the school, school district, or charter school (i.e. an annual form asking parents to confirm address).**

Every school district or charter school is required,[4] within 30 days of enrollment, to obtain a certified copy of a pupil's birth certificate or other reliable proof of the pupil's identity and age,[5] or a letter from the authorized representative of an agency having custody of the pupil pursuant to title 8, chapter 2 certifying that the pupil has been placed in the custody of the agency as prescribed by law. A school district or charter school MAY seek photo identification from the person enrolling a student to ensure that the adult is entitled to enroll the student in school, as long such a requirement does NOT unlawfully bar a student from enrolling in school.[6]

In case of an ADE Audit, the school, school district or charter school will be asked what process is used and what documentation is obtained via this process. If the student's residence has not changed, an affirmation (via a checkbox) that the previously provided proof of residency remains accurate should be sufficient. The documentation supporting Arizona residency should be maintained according to the school's records retention schedule.

For members of the armed services, a school may enroll a student if the parent provides a hard-copy or electronic document of their transfer or pending transfer to a military installation within the state. The parent must provide official documentation of residency within ten days after the arrival date which may include a temporary on-base billeting facility as their address. **PROOF OF RESIDENCY IS NOT REQUIRED FOR HOMELESS STUDENTS.**[7] 42 U.S.C.§ 11 432(g)(3)(C)(i).

In general, students will fall into one of two groups: (1) those whose parent or legal guardian is able to provide documentation bearing his or her name and address; and (2) those whose parent or legal guardian cannot document his or her own residence because of extenuating circumstances including, but not limited to, that the family's household is multi-generational. Different documentation is required for each circumstance.

1. **Parent(s) or legal guardian(s) that maintains his or her own residence:** The parent or legal guardian must complete and sign a form indicating his or her name, the name of the school district, school site, or

[4] A.R.S. §15-828.
[5] Other proof of the pupil's identity/age includes: pupil's baptismal certificate, an application for social security number or original school registration records and an affidavit explaining inability to provide a copy of the birth certificate, A.R.S. § 15-828 (A)(1)-(3).
[6] For more information, please read U.S. DOJ Civil Rights Division "Fact Sheet: Information on the Rights of All Children to Enroll in School", https://www.justice.gov/sites/default/files/crt/legacy/2014/05/08/plylerfact.pdf.
[7] Per A.R.S. §15-824 (C), "Homeless student" means a pupil who has a primary residence that is: (1) A supervised publicly or privately operated shelter designed to provide temporary living accommodations; (2) An institution that provides a temporary residence for individuals intended to be institutionalize or; (3) A public or private place not designed for, or ordinarily used as, a regular sleeping accommodation for human beings.

charter school in which the student is being enrolled, and provide **one** of the following documents, which bear the parent or legal guardian's full name and residential address or physical description of the property where the student resides (no P.O. Boxes):

- Valid Arizona driver's license, Arizona identification card
- Valid Arizona motor vehicle registration
- Valid Arizona Address Confidentiality Program authorization card
- Property deed/Mortgage documents
- Property tax bill
- Rental agreement or lease (including Section 8 agreement or off-base military housing)
- Utility bill (water, electric, gas, cable, phone)
- Bank or credit card statement
- W-2 wage statement
- Payroll stub
- Certificate of tribal enrollment (506 Form) or other identification issued by a recognized Indian tribe located in Arizona
- Other documentation from a state, tribal, or federal agency (Social Security Administration, Veterans' Administration, Arizona Department of Economic Security, etc.)
- Temporary on-base billeting facility (for military families)
- Under A.R.S. § 41-5001(A), school districts and charter schools must accept consular identification cards that are issued by a foreign government as a valid form of identification if the foreign government uses biometric verification techniques in issuing the consular identification card.[8]

*A model Arizona Residency Documentation Form is available for schools at the end of this document.

2. **Parent(s) or legal guardian(s) that does not maintain his or her own residence:** The parent or legal guardian must have an **affidavit of shared residency** form completed indicating his or her name, the name of the school district, school site, or charter school in which the student is being enrolled, and submit a signed, notarized affidavit for the person who maintains the residence where the student lives attesting to the fact that the student resides at that address, along with a document from the bulleted list bearing the name and address of the person who maintains the residence.

*A model Affidavit of Shared Residence form is available for schools at the end of this document.

USE OF AND RETENTION OF DOCUMENTS BY SCHOOLS

School officials must **retain a copy** of the attestations or affidavits and copies of any supporting documentation presented for each student (photocopies acceptable) that school officials believe establish validity. Documents presented may be different in each circumstance, and unique to the living situation of the student. Documents retained by the school district or charter school may be used as an indication of residency; however, documentation is subject to audit by the Department.

Personally identifiable information other than name and address (SSN, account numbers, etc.) should be redacted from the documentation either by the parent/guardian or the school official prior to filing. **MOST INFORMATION PROVIDED BY PARENTS AND GUARDIANS TO ARIZONA PUBLIC SCHOOLS IS AN EDUCATIONAL RECORD MADE CONFIDENTIAL UNDER THE FEDERAL EDUCATIONAL RIGHTS AND PRIVACY ACT AND ARIZONA LAW UNLESS DESIGNATED BY THE SCHOOL AS DIRECTORY INFORMATION. A PARENT OR GUARDIAN MAY OPT OUT OF DIRECTORY INFORMATION IN ACCORDANCE WITH DISTRICT POLICY. OTHERWISE, EDUCATIONAL RECORDS ARE ONLY USED FOR LEGITIMATE EDUCATIONAL PURPOSES.**

[8] See *Amphitheater Unified Sch. Dist. No. 10 v. Harte,* 128 Hart Ariz. 233, 234 (1981), § 15-187(C); noting that school districts and charter schools are political subdivisions.