# New Employee Technology Access
## Choctaw Tribal Schools

### The following process will be utilized for ANY staff member using a computer with the Choctaw Tribal Schools.

1. Principals should have the employee needing an account to fill out the attached forms
   - Systems Access Request
   - Choctaw Tribal Schools Internet Use Policy
   - NASIS Rules of Behavior **(only if a NASIS user)**

   These forms will serve as our request for a network log-in and are mandatory. All three forms require the signature of your direct supervisor.

2. Send only the forms to DOS, ATTN: Amy Pauls.

3. DOS staff will then process the request for a DOI Learn log-in.

4. Once you receive your Department of Interior (DOI) log-in, complete the "Federal Information Systems Security Awareness" course. This log-in will only be for the DOI site.

5. Once you have completed the training you should print a certificate for your own records and send a copy to Amy Pauls. Certificates can be accessed using the “View Training History” icon.

6. DOS staff will then coordinate the setup of a tribal schools email account, network login, and Infinite Campus/NASIS account. All information will be sent back to the school principal or designee.

7. If you need any further assistance please call the Data Management office at DOS (601-663-7308).

*FYI – Record your login information and keep this sheet for future reference*

You will be issued temporary passwords for the computer log-in, DOI Learn, Email and student information system. Be sure to write down the new passwords as you type them in the first time. You may receive a prompt to change your password.

## Choctaw Tribal Schools network

User _____

Password _____

## Security Awareness Test (FISSA+)

https://gm2.geolearning.com/geonext/doi/login.geo

DOI User _____

Password _____

## Choctaw Tribal School Email

http://mail.choctawtribalschools.com

User _____

Password _____

## Infinite Campus

(Student information system/gradebook)

User _____

Password _____

**CHOCTAW TRIBAL SCHOOLS**
**INTERNET USE POLICY**
**ACCEPTABLE AGREEMENT/USE POLICY**

Internet and network access is provided to the students and staff at Choctaw Tribal Schools. Education is the primary function of Choctaw Tribal Schools. Computers are tools with which to perform research, retrieve information, compile data, and create documents.

By signing the Acceptable Use Policy, the students, staff, and students' parents or guardian agree to obey the rules outlined in the Acceptable Agreement/Use Policy. This document describes responsibilities for use of the network and Internet and also consequences if privileges are abused.

The use of equipment, computers, network resources, and the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of these privileges.

Network Etiquette – Users are expected to abide by the general accepted rules of network etiquette. These include but are not limited to the following:

- Be polite. Messages should not be abusive to others.
- Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
- Do not reveal addresses, credit card numbers, or phone numbers
- Illegal activities are strictly forbidden.
- Electronic mail is not guaranteed to be private. People who operate the system have access to all mail.
- Messages relating to, or in support of, illegal activities may be reported to the authorities.
- Do not use the network in such a way that others' use of the network would be disrupted.

Users agree to abide to the following:

- Use of the network must be in support of education and research.
- Users must not reveal their password or use others' passwords.
- Users shall not damage computers, computer systems or computer networks, which include altering software components of a computer or system.
- Users are prohibited from transmitting or intentional receipt of hate mail, harassment, and other antisocial behaviors on the network.
- Users shall not use the network to access or process pornographic material, inappropriate text files, or any illegal activity.
- Students must not play games on computers unless authorized by monitoring staff member.
- Users agree not to use the chat rooms.
- Users agree not to send chain letters.
- Students shall not send, receive or check personal E-mail, except before or after school.

Computer Lab Usage

- All staff is responsible for monitoring student activity on the network. The staff members assigned to a group of students is responsible for monitoring and overseeing their network and Internet activity.
- No food or drinks in the Computer Labs.
- Teachers are expected to have plans before students use the Internet, which include preresearching sites that are used.

Consequences of Unacceptable Use

- Suspension and/or termination of network and Internet privileges.
- And/or additional disciplinary action as determined at the administrative level regarding unacceptable language and/or behavior.
- And/or referral to law enforcement authorities for criminal or civil prosecution.

**Internet Use Policy – Acceptable Agreement/Use Policy (continued)**

Respect for Others

- Users shall only use computer equipment for which they have been granted permission or that which has been assigned or loaned to them by a district or school administrator, technologist or authorized staff member, for their use. Within reason, users are responsible for repairing damage done to any computer while in their possession.
- Users shall be considerate of others when using school/district computer equipment or informational resources and abide by any time limit restrictions stated.
- Users shall log off workstations after finishing their work to protect their own privacy and ready the workstation for use by others.

## AGREEMENT SIGNATURES

User Agreement

User's Full Name (please print) _____

I understand and will abide by the terms and conditions for Internet Access. I further understand that any violation of the federal and/or state regulation is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, and school disciplinary and/or appropriate legal action may be taken.

User's Signature _____ Date _____

THIS IS A UNITED STATES FEDERAL GOVERNMENT COMPUTER SYSTEM, WHICH MAY BE ACCESSED AND USED ONLY FOR OFFICIAL GOVERNMENT BUSINESS BY AUTHORIZED PERSONNEL. UNAUTHORIZED ACCESS OR USE OF THIS COMPUTER SYSTEM MAY SUBJECT VIOLATORS TO CRIMINAL, CIVIL, AND/OR ADMINISTRATIVE ACTION UNDER 18 U.S.C. 1030 ET AL.

*Please read the following and sign below to acknowledge your acceptance of the NASIS Rules of Behavior.*

# NASIS Rules of Behavior

Rules of Behavior are part of a complete program to provide good information security and raise security awareness. ROB describe standard practices needed to ensure safe, secure, and reliable use of information and information systems.

The Rules of Behavior cover all government and non-government users of government systems. This includes contract personnel and other federally funded users.

Penalties for noncompliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

These ROB do not replace existing security policies or directives. Rather, they further supplement and articulate existing security policies and practices and are consistent with the following directives:

- DOI Departmental Manual 375, Chapter 19
- DOI Information Security Plan
- DOI Bureau of Indian Affairs Handbook
- DOI Bureau of Indian Affairs System Security Plan

1. I understand that all BIE computer systems, including electronic mail, Internet connections and associated equipment, software and data are to be used for official business and according to the Department of Interior and BIE policies only. Law forbids any other use of these items (Section 641 of 18 U.S. Code, Public Law 99-474, and other Federal Statutes and Regulations).

2. Access is granted only to authorized users. Unauthorized use of a user accounts includes, but is not limited to: the use of a user account to access systems by any person other than the authorized user; theft; damage to or corruption of the database; destruction of or tampering with information; disclosure of any sensitive information.

3. I understand that individuals are subject to having any of their activities monitored and recorded at any time. Violations of the law can result in the loss of computer privileges and disciplinary action, up to and including termination from employment and other criminal and civil penalties.

4. I will select appropriately complex passwords for use on NASIS and will NOT share my passwords with anyone else nor store them in any way that increases the probability that they will be compromised.

5. I will handle sensitive information appropriately. I will not disclose information covered by the Privacy Act to unauthorized personnel. I understand that sensitive or proprietary information is not to be exchanged, divulged, or compromised in any way unless an exchange is necessary for official government business.

6. If I become aware of a security breach or incident such as password sharing or unauthorized use of any BIE computer system, I will immediately notify my supervisor or the BIA Office of Information Security and Privacy.
7. My signature below shows my acceptance of the above responsibility for my use of NASIS. I

acknowledge that the unauthorized use of any US government computer system is punishable under Public Law 98-473. I also understand that I am accountable for any and all actions performed as a result of access to systems via my user account and that unauthorized actions may subject me to disciplinary actions.

My signature acknowledges that I have read this certification form and that I agree to protect the security of the system and its contents.

Employee Name: _____
(Printed)

Signature: _____ Date: _____

**Maintenance of Request Forms**

The school NASIS administrator is to retain the signed original of this document.