# Aaniiih Nakoda College
# Policy Standards
# Information
# Technology

# A Handbook for Students

**PASSED by ANC BOARD OF DIRECTORS, AUGUST 13, 2006**
**(Revised 8-10-06 by Harold Heppner)**
**(Revised 12-12-2016 by Harold Heppner)**

# TABLE OF CONTENTS

# Introduction

This document establishes computer usage guidelines for the Aaniiih Nakoda College (ANC). Aaniiih Nakoda College offers a wide array of computing, networking, and telecommunications resources and services to members of the college community. These services are in place to facilitate teaching and learning, research, and administrative activities and to further Aaniiih Nakoda College's mission. This document contains information technology policies and procedures and also outlines responsibilities of those who use computing and networking facilities at the college. Users of these services agree to abide by and be subject to the terms and conditions contained in this and all other applicable College policies. Some departments on campus may have additional facilities, practices, and policies that apply to use of computing facilities in those departments. These policies are designed to enable high- quality services and maximize productivity while protecting the rights of all members of the community. All students and employees of Aaniiih Nakoda College are required to read and comply with the policies laid out in this Manual (which may be amended from time to time). This manual does not attempt to anticipate every situation that may arise and does not relieve anyone of their obligation to use common sense and good judgment.

Questions or suggested improvements on these policies and procedures or other computing matters should be addressed to the Manager of Information Technology at Aaniiih Nakoda College. This handbook is posted on the IT Department web site and is reviewed every two years.

# Access to Information Technology Resources

### *Eligibility*

Information Technology Resources (computer hardware, software, telephone systems, networks, services, data, and other information) are made available at ANC to support and facilitate the teaching, research and administrative functions of the College. Access to these resources is provided to faculty, administration, staff, and enrolled students consistent with their responsibilities.

Under no circumstances may anyone use college IT resources in ways that are illegal (e.g. copyright violations), threaten the College's tax- exempt or other status, or interfere with reasonable use by other members of the College community.

Other individuals, upon submission of a request, may be granted access to some, or all, of ANC IT resources by the President of the College. The terms of access will be stated at the time access is granted.

### *Account Activation/Termination*

E-mail access at ANC is controlled through individual accounts and passwords. Each user of ANC's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee and student to protect the confidentiality of their account and password information.

### *Personal Computers on the Network*

Internet addresses are provided by IT Department. In order to obtain a static Internet (TCP/IP) computer address the owner of the system must register the computer with IT Department network services.

The rules and regulations contained in this policy pertaining to electronic mail and Internet access are equally applicable to the use of personal machines for file sharing or as servers. If bandwidth or other problems occur, IT Department reserves the right to discontinue access to the machine. Computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the College. If personal computers on the ANC network are used as servers, the administrator has the additional responsibility to respond to any use of the server that is in violation of these policies and procedures. Server administrators must take steps to prevent recurrence of such violations and report these violations to the ANC Network Administrator (postmaster@mail.ANCc.edu).

IT Department reserves the rights to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network. See Noncompliance and Sanctions for examples of these activities.

IT Department reserves the right to restrict access to the network during expansion, or for diagnostic and maintenance services. Every effort will be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

### *Virus Protection*

Aaniiih Nakoda College requires all existing and incoming students to install anti- virus software on their personal computers by the end of the second week of classes each semester. Failure to do so can result in the loss of connectivity to the Aaniiih Nakoda College network until anti- virus software is installed. AVG anti- virus software is provided free to all students. Other anti- virus products may be substituted as long as they are kept current.

### *Dial- Up Connections*

For all campus users the primary access to ANC computing services is through the campus network. Dial- in access via modem is not provided.

### *Personally Owned Equipment*

IT office also provides repair for personally owned computers. Computers are repaired at a cost rate established by ANC. There is a minimum charge for examining the equipment if repair is not needed. Equipment must be delivered to the IT office during regular business hours. IT Department will be available each day between 7 am and 5 p.m. to receive equipment, or by special arrangement by calling or by e- mail (admin1@ancollege.edu). Payment for the repairs must be made by cash, check, or money order when the equipment is picked up.

Charges for repair cannot be applied to your Aaniiih Nakoda College account.

## Electronic Mail (E- Mail)

### *Department or Group Accounts*

By special permission, college departments and student groups will be granted a single account to facilitate connections between the department or group and interested parties. The department or group must identify one person to be responsible for the account and to act as the contact person. In addition, student organizations must be registered with Student Support Services before an account will be granted.

All students of ANC are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Applications for these temporary accounts must be submitted in writing to Aaniiih Nakoda College President. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement. E-mail access will be terminated when the student or third party terminates their association with ANC, unless other arrangements are made. ANC students who have graduated from ANC will still be on ANC's Alumni E-mail system for as long as the student wants it. ANC is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their enrollment has ceased.

### *Appropriate Use of E-mail*

ANC strongly recommends that e- mail not be used for confidential communication. E- mail is now considered a formal written record that carries the same legal weight as a formal memorandum. Users of e- mail should remember that e- mail messages become the possession of the receiver and can be easily duplicated and redistributed by recipients. Messages that have been deleted can unintentionally be retained on system backup files. In addition, even secure passwords are not completely confidential. When a private message needs to be conveyed between two individuals, a conversation is the best way to accomplish it, and messages that should not be preserved should be deleted immediately.

College policy prohibits certain types of e- mail. These include email that may be perceived as harassment, political campaigning, or commercial solicitation. Chain mail is also prohibited. Violators will be subject to loss of computer access privileges, as well as additional disciplinary action as determined by the ANC judiciary procedures. Certain types of e- mail, including but not limited to harassing e- mail, may also subject the sender to civil or criminal penalties. In spite of College policy, e- mail can be abused by malicious users who know the owner's computing ID and password. Users are responsible for protecting their own passwords.

### *ListServ Lists*

ListServ is a commercial software product installed on our E- mail system. It is designed to provide an easy way to create and maintain large E- mail mailing lists. These lists can be used for the one- way distribution of information, for E- mail based discussion, questions and answers, etc. Lists are created and "owned" by an E- mail user who manages the lists behavior.

Any faculty, staff, or student member of the Aaniiih Nakoda College community is entitled to become a ListServ list owner. Campus- based organizations and departments are also entitled to own lists, but an individual within the group must be designated as the list owner. Students must be in good standing with the Dean of Students office and student organizations must be registered with Student Support Services.

All lists must be approved by the IT Department prior to creation, but the following general guidelines apply:

1.) The purpose of the list must pertain to Aaniiih Nakoda College business.

2.) Lists are not open to off- campus subscribers unless special permission is obtained. However, Aaniiih Nakoda College students or employees who use off- campus E- mail addresses are allowed to own and belong to lists.

3.) It is the list owner's responsibility to learn the commands necessary to manage the list's subscribers.

4.) Under no circumstances can a list be used to participate in or promote activities that are illegal, violate the Aaniiih Nakoda College code of conduct, or the Aaniiih Nakoda College Policy and Procedure Manual.

To apply for list ownership and select a list type, please read Becoming a ListServ List Owner from which you can create your list.

### *ListServ Mass Mailing Lists*

As a service to the Aaniiih Nakoda College community, several E- mail based mass mailing lists have been created. These are designed to facilitate the timely and cost- effective distribution of information to the campus community. E- mail now reaches almost all faculty, administration and staff and students. Participation in the mass mailing lists is voluntary.

In order that these lists remain a reliable means of communication, it is important that members of the ANC community abide by a few guidelines. These guidelines are not designed to limit free speech but are intended to keep your mail volume at a reasonable level.

Most importantly, anonymous mailings are prohibited. The sender's real name must be identified (in full) within the body of the message - not just at the top in the "from" line. The mass mailing lists are intended for:

1. Announcement of campus events and deadlines

2. Changes in campus policies, procedures, organizations, or

departments

3. Notification of the availability of services and/or facilities

Any individual wanting to post a message to the mass e- mail lists that falls outside of the guidelines, but is felt to be of vital importance to the community, must send a request for an exception to: The request will be directed to the appropriate college official (Dean of Students, Dean of Academics, President). If the exception is approved the message will be posted by that college official. Approval or denial will be communicated to the person making the request. Examples of such exceptions might include reports of inappropriate behavior, including campus vandalism, and racist, sexist, or other acts against members of the community.

Please consider your audience carefully (e.g., do not send a mailing to all employees if you only need to reach faculty and students). These lists are NOT intended for messages of a personal nature. Examples of inappropriate uses include, but are not limited to:

1. Soliciting support (financial or otherwise) for charity or special causes not connected with a College effort

2. Personal opinion, public debate, or campaigning

3. Give- aways (personal property such as furniture, tickets, equipment, books, etc.)

4. Unverified public service announcements (such as virus alerts, unsafe products, etc.)

5. Chain mail

6. Services offered or services sought (except for College related services)

7. Lost and found (except when it is Aaniiih Nakoda College property, or involves animals)

8. Items for sale - or items desired (including houses, tickets, books, services, etc.)

9. Rides

### *Penalties for Violations*

Any violation will be sent to the appropriate referral person. First, Dean of Students, if it can not be solved there, onto Dean of Academics with Dean of Students, if it can not be solved there, onto ANC Executive Committee and President has the authority for penalties.

### *Licensing of Software*

The use of all software in the College is protected by copyright laws and must be used in accordance with software licenses. It is against College policy to copy or reproduce any licensed software. Unlicenced software may not be installed on any computers owned by ANC. The unauthorized use or copying of software is a serious violation of policy and subject to disciplinary action. Such unauthorized use or copying may also subject the offending individual to lawsuits by third parties.

### *Software on Personally Owned Equipment*

ANC educational licensing agreements for software specifically limit installation to machines owned by the college. Therefore, software purchased by ANC under these agreements may not be installed on personally owned equipment. Our current license agreement with Microsoft does allow the installation of one copy of Microsoft MSDNAA on the home machine. For information on these programs, ANC current licensing agreements, and exceptions, contact the Director, IT Department.

## Security

### *Security On Data Networks*

Security for access to the data network and to files or applications on a server is implemented via user ID and password systems. Each user is responsible for all e- mail transactions made under the authorization of his or her ID and password, and for all network e- mail activity originating from that connection. Users are personally responsible for the security of the ID and password assigned to them. Viewing, copying, altering or destroying any file, or connecting to a computer on the network without explicit permission of the owner is prohibited. Users may not use the ANC data network or telephone system to attempt to circumvent protection schemes or exercise security loopholes in any computer, network, or telephone system component.

### *User IDs and Passwords*

Passwords should be known only to the person responsible for the account and user ID. Ways to ensure this include avoiding storing passwords or any other information that could be used to gain access to other computing resources on your workstation, never sharing passwords, and never taping passwords to a wall, under a keyboard, or in other easily discoverable areas. Access to user IDs may not be loaned or sold and any suspected breach of password security should be immediately reported to the IT Department e- mail administrator. Passwords should be changed (at least) every six months.

### *Protecting Desktop Equipment and Files*

Backups and protection of files stored on desktop equipment are the responsibility of the user of that equipment. Users must back up their work files on a regular basis. Department members are responsible for ensuring that critical files are backed up in their areas. (see appendics)

Individual users are responsible for safeguarding the equipment entrusted to them by the college. This includes reasonable protection of equipment from damage and theft. Individual users are also responsible for safeguarding any equipment they own personally and bring to campus.

### *Confidentiality and Privacy*

ANC takes reasonable steps to protect users from unauthorized entry into their accounts or files, whether by other users or by system administrators, except in instances where a system- related problem requires such entry. A limited number of authorized ANC personnel must occasionally monitor information on the network and/or computer systems to maintain the integrity of the systems. This access is required for reasons that include, but are not limited to, trouble- shooting hardware and software problems; preventing unauthorized access and system misuse; providing for the overall efficiency and integrity of the systems; protecting the rights and property of the College; ensuring compliance with software and copyright, distribution, and other College policies concerning the use of the computer network; and complying with legal and regulatory requests for information.

System monitoring is a mechanism for keeping track of computer system activities, rather than a method for accessing private information. IT Department personnel also take reasonable steps to prevent the dissemination of information concerning individual user activities. It is the policy of IT Department to disclose neither the contents of electronic mail and data files stored in or transmitted via the College Computer System nor the activities of individuals on the campus network to other individuals within or outside the College community in the absence of a court order, or other legal mandate, or permission of the owner.

Private communication via computer is treated with the same degree of protection as private communication in other media. However, due to limitations of current technologies, which are inadequate to protect against unauthorized access, the confidentiality of e- mail and other system files can not be assured. All users should be aware of this and use reasonable caution when transmitting confidential materials.

### *Central Computer Operations*

Access to computer operations areas is restricted to those responsible for operation and maintenance. Computing facilities on campus are secured when not open for business. IT Department takes action to provide reasonable protection against environmental threats such as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power for central server and network facilities. IT Department maintains procedures for protecting critical data that reside on central servers.

While ANC provides security for files stored on central computing facilities, ANC cannot be responsible for protection against floods, fires, and catastrophic events of this type. Backup files from central servers are kept for only a few days. IT Department does not guarantee the availability of backups for the restoration of files deleted through user error.

### *Responsible Use of Networks and Computing Facilities*

Aaniiih Nakoda College is a public institution fully committed to the ideals of academic freedom, freedom of expression, and cultural diversity. At the same time, inappropriate behavior and malicious misuse of computing resources that in any way degrades the College equipment and services or violates the rights of others in the community is strictly prohibited.

### *Individual Responsibility*

While IT Department is responsible for monitoring the use of computer systems, it is also the responsibility of all individuals in the ANC community to urge their peers and colleagues to use the network and systems appropriately. This is the only way that the integrity and availability of the network and systems can be ensured for everyone. Each member of the community is responsible for using only those accounts or computers for which he or she has authorization and is responsible for protecting all passwords. Individual responsibility includes respecting the rights of other users. Individuals are urged to report unauthorized use of computers, networks, or other IT Department facilities on campus by calling the IT Department e- mail administrator or notifying the Information Technology Department.

### *Logging In*

All students, employees, and individuals will may see the below message each time they log into a computer.

***This is a private computer system and is the property of Aaniiih Nakoda College. It is for authorized use only. Users have not explicit***

***or implicit expectation of privacy. Any or all users of this system maybe be intercepted, monitored, recorded, copied, audited, inspected and disclosed to management and law enforcement personnel if applicable. By using this system, the user consents to the aforementioned practices at the discretion of management. Unauthorized or improper use of this system may result in administrative disciplinary action and or civil and criminal penalties. By continuing to use this system you indicate you are aware and consent to these terms and conditions of use. <u>DO NOT LOGON if you do not agree to the conditions stated above.</u>***

### *Institutional Privileges*

Aaniiih Nakoda College reserves the right to allocate resources in different ways in order to achieve maximum usage. To accomplish this, the system administrators may suspend or terminate privileges of individuals without notice if malicious misuse or use inconsistent with this policy, any other College policy, or applicable law is discovered. Privileges may also be suspended, without notice, to meet time dependent, critical operational needs. System administrators may also limit the number of messages or files that each user has in order to keep the system functioning.

### *Legal Compliance*

All existing federal and state laws and College regulations and policies apply to the use of computing resources and all users of such resources are required to be in compliance with all laws, regulations and policies at all times. This includes not only those laws and regulations that are specific to computers and networks, but also those that apply generally to personal conduct.

## Copyright on Digital Information Systems

### *Introduction*

Individuals using computers and networks ("Digital Information Systems") at Aaniiih Nakoda College (the "College") are responsible for complying with copyright laws and the College's policies and procedures regarding use of the Digital Information Systems. The College reserves the right to deny, limit, revoke or extend computing privileges and access to the Digital Information Systems in IT Department discretion. In addition, alleged violations of this procedure, the College's policies regarding use of the Digital Information Systems, or other policies of the College in the course of using the Digital Information Systems may result in an immediate loss of computing privileges and may also result in the referral of the matter to the College's judicial system or other appropriate authority.

The procedures outlined below will apply when the College receives notification of an alleged copyright infringement. For purposes of these procedures, an E−mail message shall be considered a written notice or request.

### *Notification of Infringement*

1. Copyright holders who believe their copyrighted material has been infringed by an account holder must notify the College's President of the allegedly infringing action or material in writing. The notification must:
   a) identify the copyrighted material being infringed in sufficient detail to permit the College to locate the allegedly infringing material on the College's Digital Information Systems,
   b) state the basis for the claim of possible infringement,
   c) state the basis for the copyright holder's copyright in the work (e.g., author, owner, assignee).

2. The Designated Agent will notify the account holder who appears to have posted the allegedly infringing material, and will investigate the complaint promptly.

3. If, after conducting an investigation, the IT or Designated Agent determines that the allegedly infringing material appears to infringe the copyright of the copyright holder, the Designated Agent will follow the procedures for Removal of Infringing

Material set forth below.

### *Removal of Infringing Material*

In the event that the allegedly infringing material is being used for an active class at the College, the Designated Agent will attempt to work out an arrangement with the copyright holder for use of the allegedly infringing material by the account holder until the end of the current semester. Failing a satisfactory arrangement, the Designated Agent will conduct an investigation of the incident and take action as set forth below regarding any allegedly infringing material.

If, after the Designated Agent's investigation, the Designated Agent determines that the allegedly infringing material appears not to infringe the copyright of the copyright holder, the Designated Agent will notify the copyright holder and the account holder of the determination. If the copyright holder disagrees with the determination of the Designated Agent, the copyright holder may request in writing that the College ask IT Department attorney's to render an opinion as to whether the allegedly infringing material constitutes copyright infringement pursuant to paragraph below.

If, after the Designated Agent's investigation, the Designated Agent determines that the allegedly infringing material appears to infringe the copyright of the copyright holder, the Designated Agent will notify the President for Information Technology, Aaniiih Nakoda College, the copyright holder and the account holder whose account was used to post the allegedly infringing material.

Upon receipt of such notification from the Designated Agent, the President Aaniiih Nakoda College, will direct the appropriate IT Department staff member to remove, or block access to, the allegedly infringing material.

Upon receipt of notification from the Designated Agent that the allegedly infringing material appears to infringe the copyright of the copyright holder and is being blocked or removed from ANC Digital Information Systems, the account holder may request that the

Designated Representative restore the removed or blocked material based on the account holder belief that the allegedly infringing material is not infringing. Such request must be in writing and include a detailed statement of the basis for the account holder's belief that the allegedly infringing material is not infringing, as well as a request that the removed or blocked material be restored.

If the Designated Agent receives such request from the account holder, the Designated Agent will provide a copy of the request to the copyright holder.

If, within 10 days after a copy of the account holder's request is sent to the copyright holder by the Designated Agent, the Designated Agent has not received a written request from the copyright holder to continue the blocking or removal of the allegedly infringing material, the Designated Agent will notify the President for Information Technology, Aaniiih Nakoda College to restore the material. The President for Information Technology, Aaniiih Nakoda College, will restore the allegedly infringing material within four days after receipt of such notification.

If the Designated Agent receives within 10 days a written request from the copyright holder to continue the blocking or removal of the allegedly infringing material is received from the original sender, the Designated Agent will provide copies of all correspondence in the matter to the President for Information Technology, Aaniiih Nakoda College, who will forward copies of such correspondence to the College's attorneys, who will be asked to render an opinion as to whether the allegedly infringing material constitutes copyright infringement. If the allegedly infringing material is determined not to constitute copyright infringement, the material will be restored by the President for Information Technology, within four days of such determination.

### *Designation of Agent to Receive Notification of Claimed Infringement*

This is to notify copyright holders that Aaniiih Nakoda College's Designated Agent to receive notices and requests concerning claimed infringement, pursuant to the Digital Millennium Copyright Act, is President. Any copyright holder wishing to send a notice to Aaniiih

Nakoda College regarding possible copyright infringement should file that notice in writing with President at the following address:

President
Aaniiih Nakoda College
BlackFeet Street
PO Box 159
Harlem, MT 59526
Telephone: 406-353-2607
Fax: 406-353-2898

### *Indemnification of Aaniiih Nakoda College*

Users agree, in consideration of access to the College's computing, networking and media services, to indemnify, defend, and hold harmless the College for any lawsuits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the College's computing, networking, and media services and facilities.

### *Noncompliance and Sanctions*

Information Technology Services may suspend or terminate all computing privileges of any individuals without notice who engage in improper computing activities. Serious cases, as determined by the President of Aaniiih Nakoda College, will be referred to the Board of Directors for disciplinary action. Such disciplinary action may include the suspension, expulsion, or termination of the offending individual, as appropriate and as determined at the sole discretion of Aaniiih Nakoda College. Where violation of state and federal law is involved, cases will be referred to the proper legal authorities for action. The following serves to provide examples of violations of computing or computing facility policies at Aaniiih Nakoda College. The list of violations includes, but is not limited to:

### *Malicious misuse. Examples*

Using IDs or passwords assigned to others, disrupting the network, destroying information, removing software from public computers, spreading viruses, sending e−mail that threatens or harasses other people (**Class A -** misdemeanor under Montana State law), invading the privacy of others, and subscribing others to mailing lists or providing the e−mail addresses of others to bulk mailers without their approval.

### *Unacceptable use of software and hardware*

Examples: knowingly or carelessly running or installing unlicensed software on any computer system or network; giving another user a program intended to damage the system; running or installing any program that places an excessive load on a computer system or network, or compromises the security of the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.

### *Inappropriate access*

Examples: unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus network to gain unauthorized access to any computer system; connecting unauthorized equipment to the campus network; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data); knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks; deliberately wasting or overloading computing resources, such as printing too many copies of a document; or other activities.

### *Inappropriate use of electronic mail and Internet access*

E−mail communications are subject to statements of conduct as published in the Student, Faculty, Administrator, Staff, and Maintenance and Operations Handbooks, as well as all applicable federal and state laws. In addition, other activities that threaten the integrity of the system or harm individual users are not allowed. These include, but are not limited to initiating or propagating electronic chain letters; inappropriate mass mailing including multiple mailings to news groups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication or sending anonymous e−mail; using another person's e−mail account or identity to send e−mail messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; or using e−mail or personal web page advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.

### *Reporting Critical Service Outages During An Academic Term*

During normal business hours (Monday − Friday, 8:00 a.m. - 5:00 p.m.), members of the College community should notify the IT Department of suspected problems with computers, networks, and related information technology resources. IT will investigate the problem and determine corrective action. If the IT staff determines that the problem is related to the campus network or a server, they will take appropriate action. Resolution of critical service outages (defined below) will be a top IT Department priority and will be resolved in a timely manner. Non−critical problems will be investigated and resolved as soon as is feasible.

Outside of business hours and on college holidays suspected critical service outages should be reported by email or phone calls.

Any suspected critical service outages should be reported to the Department Head on duty in the Aaniiih Nakoda College Lab. The student will follow prescribed diagnostic routines to determine if the problem is indeed of a critical nature. If so, s/he will call the appropriate IT Department staff member to resolve the problem.

A critical service outage is defined as one or more of the following:

1. Failure of the campus network equipment or Internet connection

making it impossible for a majority of users to access on campus or off campus resources.

2. Campus wide printing failure (not individual printers).

3. Failure of a majority of computers in a public computer lab.

4. Failure of the campus web server affecting the entire campus.

5. Failure of the campus telephone system making it impossible for a majority of users to make outgoing calls or receive incoming calls.

6. Failure of the college e−mail system affecting the entire campus.

7. Failure of the college administrative system affecting the entire campus.

## Chain of Command

All violations will be report to the IT Department, then to Dean of Students, and if need be, Dean of Students will report to the President who has the final decision.

## *AANIIIH NAKODA COLLEGE'S INFORMATION TECHNOLOGY USER AGREEMENT*

I have read and understand the INFORMATION TECHNOLOGY HANDBOOK. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to the Aaniiih Nakoda College Code of Conduct policy.

Name:_______________________________________________

Signature:____________________________________________

Date:________________________________________________