



**Diné College**

---

**Information Technology  
Policies Manual**

---

### **Information Technology Department Operational Statement**

The Information Technology Department's mission is to work in partnership with members of the Diné College Community to facilitate their use of computing, voice, video, and network resources.

To advance Diné College's institutional mission and strategic goals, we endeavor to empower students, faculty and staff to effectively utilize technology resources by striving to provide high standards of support services and infrastructure.

---

Information Technology  
Policy and Procedure Manual

Table of Contents

Policy: **INTRODUCTION** ..... 5

    A. Permission ..... 5

    B. Definitions..... 5

    C. Policy Maintenance ..... 5

    D. Applicability of Policy ..... 6

    E. Sanctions ..... 7

Policy: **USE OF DINÉ COLLEGE INFORMATION TECHNOLOGY RESOURCES POLICY** ..... 8

    A. Goals ..... 8

    B. Responsibilities ..... 8

    C. General Exceptions..... 9

    D. Prohibited Uses ..... 9

Policy: **USE OF THE DINÉ COLLEGE NETWORK AND DATA MANAGEMENT SYSTEMS POLICY** .. 12

    A. Goals ..... 12

    B. Prohibited Use ..... 12

    C. Responsibilities ..... 13

Policy: **COPYRIGHT INFRINGEMENT POLICY** ..... 14

    A. Technology-Based Deterrent ..... 14

    B. Community Education ..... 14

    C. Procedures for Handling Unauthorized Distribution of Copyrighted Material..... 14

    D. Offering Alternatives..... 14

Policy: **EMAIL USAGE POLICY** ..... 16

    A. Prohibited Use ..... 16

Policy: **INTERNET USAGE AND SOCIAL MEDIA POLICY** ..... 18

    A. Purpose ..... 18

    B. Internet Usage Policy ..... 18

    C. Social Media Policy..... 20

Policy: **INFORMATION TECHNOLOGY SECURITY POLICY** ..... 22

    A. Responsibilities ..... 23

    B. Security Breach Notification Procedure ..... 23

Policy: <b>INFORMATION TECHNOLOGY SECURITY PLAN</b> .....	26
A. Designation of Representative: .....	26
B. Scope .....	26
C. Elements of the IT Security Plan .....	26
D. Adjustment to IT Security Plan .....	28
Policy: <b>COMPUTER LABS POLICY</b> .....	29
A. Prohibited Use .....	29
B. Access to Computing Labs .....	30
C. Labs and Classrooms.....	30
D. Sensitive Materials .....	31
E. General Lab Rules.....	31
F. Responsibilities .....	33
Policy: <b>USE OF DINÉ COLLEGE INFORMATION TECHNOLOGY RESOURCES BY THIRD PARTIES POLICY</b> .....	34
A. Authority.....	34
B. Permission for Temporary Use .....	34
C. Limitations on Use.....	34
D. Security Rights.....	34
Policy: <b>SOFTWARE LICENSING COMPLIANCE POLICY</b> .....	36
A. Software Licensure.....	36
B. Authority.....	36
C. Permission .....	37
D. Prohibited Use .....	37
E. Ownership.....	37
F. Violation Indemnification .....	37
G. Responsibilities .....	37
Policy: <b>TECHNOLOGY HARDWARE AND SOFTWARE ACQUISITION POLICY</b> .....	39
A. Purpose .....	39
B. Responsibilities .....	39
Policy: <b>TECHNOLOGY HARDWARE AND SOFTWARE REPLACEMENT AND UPGRADE POLICY</b> ..	41
A. Purpose .....	41
B. Responsibilities .....	42
C. Plan Statement.....	42

D. Software Upgrades ..... 44

E. Replacement Requirements ..... 44


Policy: **PRINTER STANDARDIZATION POLICY** ..... 45

**Appendix A - Definitions** ..... 46

**Appendix B - IT Policy Agreement** ..... 48

Last Revised on July 12, 2018

**Page intentionally left blank**

 <p style="text-align: center;"><b>Information Technology Policies Manual</b></p>	<b>Section 100.01</b>
	Policy: <b>INTRODUCTION</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: INTRODUCTION</b>	
Reference:	

The use of Information Technology is one of the keys to effective and efficient productivity, enabling staff, faculty and students to achieve their goals through all methods that are made available. These ever-broadening capabilities allow Diné College to extend Higher Education to those who would not otherwise have the opportunity to attend. Information Technology at Diné College permeates every campus facility for the productivity and security of all who use it. The purpose of this policy is to establish an overall framework for guiding the growth and use of our Information Technology resources in accomplishing the broader goals of Diné College.

The IT policy supplements the Diné College Personnel Policy and Procedures Manual and is enforceable through Section 900.05 Policy: Conduct and Discipline and the Student Code of Conduct - Student Discipline section.

**A. Permission**

It is not the intent of these policies to unduly interfere with educational and research use of the network or to limit academic freedom in any way, but to provide an appropriate framework for the proper exercise of those freedoms. Furthermore, it is not the intent of these policies to impinge on the intellectual property rights of authorized users.

Diné College employees and students who comply with this policy may:

1. Use Diné College owned computers, software and data to which each individual has authorized access;
2. Use the Diné College network, including access to the Internet;
3. Use computing and networking facilities and resources in a manner that is consistent with the mission and educational purpose of Diné College.

**B. Definitions**

All definitions are included in Appendix A of this Policy.

**C. Policy Maintenance**

Diné College will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to review the effectiveness of these policies and, if necessary, to modify and amend some sections of the policies and procedures, or to add new procedures.

The primary responsibility for maintenance and administration of this policy rests with the Director of Information Technology Department (ITD). ITD is responsible for drafting any updates and changes to the policies and procedures, which are to be reviewed and approved by the Director of Human Resources (DHR) and the Vice President of Administration and Finance. If both the DHR and Vice President of Administration and Finance approve the changes, , the changes will become effective and implemented upon subsequent approval from the Diné College Board of Regents. ITD will publish and announce the new or revised policy. Some policy revisions or additions may require the signatures of each employee acknowledging notice of the revised policy.

#### D. Applicability of Policy

This policy applies to all Diné College employees, students and/or non-employees who may be authorized to use Diné College Technology Resources as defined by this policy. They shall be required to agree and adhere to these policies before being granted permission to access these resources.

This policy applies to all campus facilities, equipment and services that are managed by the Diné College Information Technology department, including off-site data storage, computing and telecommunications equipment. This policy also applies to application-related services purchased from commercial cloud services, and Internet-related applications and connectivity.

Diné College users shall also apply this policy when using Diné College technology resources to navigate through networks or computing systems beyond the local systems.

Use of the Diné College technology resources shall be for the purpose of facilitating the exchange of information and furtherance of education, research, and administering missions of the college. The use of Diné College technology resources will be consistent with the purposes and objectives of Diné College.

All computer equipment may or may not be attached to the Diné College network. However, to protect these resources from misuse and/or accidental damage, these resources will still be set up by ITD technical support personnel to require the use of login accounts. The same procedures for requesting network login accounts will be followed for this type of resource, despite their lack of actual network connectivity.

Diné College Information Technology Resources that are covered under this policy, but is not limited to, the following:

1. LAN and WAN network equipment and appliances
2. Servers, blade centers and virtual server appliances
3. Server operating systems and data base management software
4. Print servers and enterprise printers

5. Distance Learning Equipment
6. Enterprise VoIP systems and phones
7. Enterprise Applications and educational learning systems
8. Wireless equipment


This Plan applies to all college-owned workstations, laptop computers, apple computers, desktops, tablets, peripherals (printers, scanners, projectors, and interactive whiteboards if applicable), network hardware (servers, switches, routers, bridges, and other key network devices), cable plant and physical infrastructure, and the institution-wide software, including operating systems, office productivity products and other site-licensed desktop applications running on those devices.

#### E. Sanctions

Violation of any of the provisions of this, or any Diné College IT policy or procedure will be dealt with immediately and may result in disciplinary action as stated in the Personnel Policy and Procedures Manual and Student Code of Conduct. The full range of disciplinary actions is available, including, but not limited to:

1. Permanent loss of computer use privileges;
2. Denial of future access to Diné College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the DHR (for employees) or the Dean/Provost/Vice President of Student Success (for students);
4. Dismissal from the college; and/or
5. Taking legal action
6. Reporting a local, state, or federal criminal offense to local authorities.



	<b>Information Technology Policies Manual</b>	<b>Section 200.01</b>
		<b>Policy: USE OF DINÉ COLLEGE INFORMATION TECHNOLOGY RESOURCES POLICY</b>
		Adoption date: July 24, 2018
		Effective date: July 24, 2018
<b>SUBJECT: GENERAL USE</b>		
Reference:		

Diné College owns all College computing systems and applications. This policy is intended to provide campus users with guidelines for responsible and appropriate utilization of these College computing and technology resources. This policy supplements the Diné College Personnel Policy and Procedures Manual. Rapid change in technology is perpetual and Diné College reserves the right to determine, at any time, what constitutes appropriate use of technology resources covered in this policy.

Diné College is responsible for overseeing the appropriate use of College Technology Resources and ensuring compliance with tribal, state and federal law. This policy is intended to provide College employees, students, and other users of these resources with guidelines for responsible and appropriate use. Additional policies, procedures and standards may also apply to the use of computer assets.

This policy assumes that all Diné College employees and students will act honestly, responsibly and with good judgment to protect these resources and to fulfill the responsibilities of proper ethics.

**A. Goals**

The goals of the use of Diné College computers policy are to:

1. Help assure the integrity and reliability of the Diné College internal networks, hosts on those networks and any computing resource connected to them;
2. Ensure the security and privacy of the Diné College computer systems and networks;
3. Ensure the protection and retention of sensitive College data;
4. Establish appropriate guidelines for the use of Diné College-owned technology on and off- campus.
5. Effectively combat the unauthorized distribution of copyrighted material by users of Dine College's network, without unduly interfering with educational and research use of the network.

**B. Responsibilities**

All users of the Diné College network have a responsibility to comply with this policy and to understand their responsibilities. This includes the requirement for confidentiality, retention and access to records detailed there.

1. Confidentiality, Retention and Access to Electronic Records

- a. All Diné College employees should be aware that electronic mail, facsimile transmissions, and voice mail are technologies that may create an electronic record. An electronic record is reproducible and, therefore, could ultimately be disclosed to third parties. Such records are considered writings and all writings may be disclosed for audit or legitimate Diné College operational or management purposes. Whatever an employee sends or receives on a College e-mail account is the property of the College and can be accessed or viewed by the College without notice. All records and information generated and stored on electronic message systems is kept according to appropriate e-mail retention schedules. *See* E-Mail Retention Policy, Section VII.B.
  - b. Education records of students attending the College are confidential and can only be released in accordance with the Family Education Rights and Privacy Act of 1974 (FERPA) and the administrative rules of the College. *See* <https://www.dinecollege.edu/admissions/student-right-to-know-act/>, Questions about student records should be referred to the College's Vice President of Student Services.
2. Logging and Monitoring
- a. Diné College has the right to log and monitor employee use of the Diné College Information Technology Resources and to ensure their appropriate use for business-related privileges. This may include, but is not limited to, review of employee computers, file server space, user accounts and all electronic documents. Diné College employees should not expect privacy in their use of Diné College state resources.

#### C. General Exceptions

The use of Diné College resources shall be for the purpose of facilitating the exchange of information and furtherance of education, research, and administration of missions of the college. Employees may not use Diné College resources, including any person, money or property, for private benefit or for the personal gain of the employee or any other person. However, employees may make occasional, but limited, personal use of Diné College Information Technology resources only if all the following conditions are met:

- a. There is little or no cost to the College
- b. Any use is brief in duration and occurs infrequently.
- c. The use does not interfere with the performance of the employee's official duties;
- d. The use does not disrupt other employees and does not obligate them to make a personal use of resources; and
- e. The use does not compromise the security, privacy, or integrity of the College network, information, or software.


#### D. Prohibited Uses

The use of Diné College Information Technology Resources is strictly intended for use by Diné College employees. This prohibits others, such as family

members and friends, from using Dine College Information Technology Resources for any purpose. Additionally, the College specifically prohibits certain use by anyone, including employees, including:

1. Any use for the purpose of supporting, promoting or soliciting for an outside organization, group, business, political candidate, or political party, unless provided for in this policy under general exceptions or authorized by the Diné College President or designee.
2. Use that promotes personal business or financial interests.
3. Any use that constitutes political campaigning or lobbying, whether for an individual, a private business, a non-profit organization or a political party, except as noted below. This includes participating in or assisting in an effort to lobby the state legislature, a state agency head, or any governmental entity.
4. Solicitation of contributions using the Diné College Information Technology Resources for political purposes.
5. Use for advocacy of personal beliefs including, but not limited to, those related to political policies and religious organizations and religious ideologies.
6. Commercial uses, such as advertising or selling.
7. Use of Diné College e-mail distribution lists for personal purposes.
8. Use for any illegal or unethical activity.
9. Use for infringement of copyrights or any intellectual property rights.
10. Any form of harassment, including sexual and racial harassment.
11. Discrimination on the basis of race, creed, color, marital status, religion, sex, national origin, age, veteran's status, sexual orientation or because of the presence of any disability.
12. Accessing, downloading or disseminating any information that a reasonable person would deem inappropriate for the workplace, such as pornography or racist materials. This restriction does not prohibit such access or retention of such materials if they are being used solely for a specific academic purpose.
13. Downloading software or files via the Internet for personal use.
14. Any activity using excessive network band-width, such as downloading music. Such activity is prohibited, even if the use is brief in duration or occurs infrequently, because it compromises Diné College's network and legitimate business activities. However, this prohibition does not apply to students when being done as directed by a faculty member for specific educational purposes.
15. Private use of any Dine College Information Technology Resources removed from Diné College, even if there is no cost to the College.
15. Hacking, attempting to subvert or assisting others to breach the security of any Diné College network or Information Technology Resources, or to facilitate unauthorized access;
16. Use of any Diné College Information Technology Resources to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, malware);
17. Participating in activities involving disclosure or masquerading;

18. Viewing, copying, altering or destroying data, software, documentation or data communications belonging to Diné College or to another individual or entity without permission;
19. Allowing another individual (whether they might otherwise be authorized to use the Diné College Information Technology Resources or not) to use a login account password.

 <p style="text-align: center;">Information Technology Policies Manual</p>	<b>Section 200.02</b>
	Policy: <b>USE OF THE DINÉ COLLEGE NETWORK AND DATA MANAGEMENT SYSTEMS POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: GENERAL USE</b>	
Reference:	

Diné College owns the Diné College Information Technology Resources including the network systems and applications. This policy is intended to provide Diné College network users with guidelines for responsible and appropriate utilization of these resources. Use of the Diné College network and Diné College data management systems shall be for the purpose of facilitating the exchange and storage of information, including information on students and/or employees, and compliance with and furtherance of, the education, research, and administrative missions of the college.

Diné College reserves the right to determine at any time what constitutes appropriate use of the Diné College network and any computing access and services provided by Diné College.

**A. Goals**

The goals of this policy are to:

1. Assure the integrity and reliability of the College internal networks, systems on those networks, databases, legacy systems, web-accessible resources, and any computing resource connected to them.
2. Ensure the security and privacy of the College computer systems, networks and data.
3. Ensure the protection and retention of sensitive data.
4. Establish appropriate guidelines for the use of the College network and data, whether accessed from on or off-campus.

**B. Prohibited Use**

Specifically prohibited uses of the Diné College network and data management systems include:


1. Hacking, attempting to hack, or assisting others to hack or breach the security of any Diné College data, network, or technology resource, or to facilitate unauthorized access;
2. Use of any Diné College network or data management system to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses, malware);
3. Viewing, copying, altering or destroying data, software, documentation or data communications belonging to Diné College or to another individual without permission;

4. Individuals allowing another individual (regardless of whether they might otherwise be authorized to use the Diné College network and/or Diné College data management systems) to use their login account password;
5. Accessing data for any purpose other than to perform the official duties of a Diné College position;
6. Unauthorized disclosure of information to a third party;
7. Bypassing the Diné College data management systems “time-out” feature, unless specifically authorized by the Director of Information Technology.

C. Responsibilities

All users of the Diné College Information Technology Resources, including its network and data management systems, have a responsibility to comply with this policy and to understand their responsibilities and all expectations as spelled out in their job duties. This includes the requirement for confidentiality, retention and access to records stored within the College systems.

Diné College ITD and its representatives also have responsibilities under this policy. These include the responsibilities for logging and monitoring networks, data management systems and electronic messaging systems.

 <p style="text-align: center;">Information Technology Policies Manual</p>	<b>Section 200.03</b>
	Policy: <b>COPYRIGHT INFRINGEMENT POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: GENERAL USE</b>	
Reference:	

It is the policy of Dine College to fully respect all rights that exist in any material protected by the copyright laws of the United States while also encouraging usage of the material that furthers the educational mission of Dine College. This Policy provides guidance to faculty, staff, and students on the usage of copyrighted material.

A. Technology-Based Deterrent

Dine College uses software to manage bandwidth utilization on campus.

B. Community Education

All students are given the opportunity to attend a session at orientation on current technology issues. This session addresses copyright infringement and other common policy violations that result through technology.

At the start of school year an email is sent to all currently enrolled students from the ITD. This email provides a number of notifications in compliance with federal and state regulations. Dine College includes in this annual notification a section on federal copyright law and the implications of copyright infringement utilizing campus technology resources.

C. Procedures for Handling Unauthorized Distribution of Copyrighted Material.

Upon receiving notification of copyright infringement through a takedown notice, ITD has a set procedure of enforcement. The infringing user is identified. First time offenders are disconnected from the network and sent a notification of infringement as well as a request to agree not to share copyright material on the network without proper permission. The user is afforded the opportunity to meet in person to discuss the takedown notice. The user may be disconnected up to two weeks. During the disconnection period students still have access to the network using lab and checkout workstations. Further infringement violations will be referred to the disciplinary procedure. Dine College disallows the sharing of copyrighted material.


D. Offering Alternatives

There are legal alternatives to unauthorized downloading that can be found at this page.

<https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/educause-policy/legal-sources-onli>





 <p style="text-align: center;"><b>Information Technology Policies Manual</b></p>	<b>Section 300.01</b>
	Policy: <b>EMAIL USAGE POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: SPECIFIC USE</b>	
Reference:	

Electronic mail tools are provided to Diné College employees and students in order for them to efficiently communicate. A number of Diné College IT security standards are in place to define the practices, processes and controls related to using Diné College-provided e-mail resources. In order to ensure that the integrity and reliability of the Diné College internal networks are not compromised by inappropriate use, users will comply with all provisions of these standards.

Email from any Diné College computer system shall not be used to create or distribute any content that is:


- Disruptive
- Offensive
- Derogatory
- Malicious
- Discriminatory about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and/or practices, political beliefs or national origin.
- Otherwise in violation of any binding law or Dine College policy.

**A. Prohibited Use**

1. Unauthorized distribution of copyrighted material.
2. Sending discriminatory, harassing or threatening messages or images;
3. Sending content that is deemed to be offensive, including the use of vulgar or harassing language/images;
4. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
5. Sending, receiving, or accessing pornographic materials;
6. Sending malicious emails, i.e. any information that could be used to sabotage institutional progress or as personal attacks;
7. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate College purposes;
8. Sending unauthorized copies of College files or other College data;
9. Destroying, deleting, erasing, or concealing College emails intended for legitimate College business;
10. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise

- harm either the College's networks or systems or those of any other individual or entity;
11. Becoming involved and promoting in partisan politics;
  12. Causing congestion, disruption, disablement, alteration, or impairment of College email systems.
  13. Using email to promote recreational games or Ponzi schemes;
  14. Hacking into another user's email account;
  15. Engaging in private or personal business activities;
  16. Extensive personal use or for personal gain
  17. Use that is in violation of any binding law or Dine College policy.

If there are questions about what is considered prohibited use, employees should check with ITD, the HRD or External Affairs Department.

 <p style="text-align: center;"><b>Information Technology Policies Manual</b></p>	<b>Section 300.02</b>
	Policy: <b>INTERNET USAGE AND SOCIAL MEDIA POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: SPECIFIC USE</b>	
Reference:	

**A. Purpose**

Diné College operates an internal private network as part of its business infrastructure. It also extends and operates external connections to the Internet. The purpose of this policy is to clearly delineate the limitations of Internet use available through that network.

Diné College’s Internet access is through a private network provided exclusively for the benefit of Diné College students, employees, staff, visitors, invitees and others directly involved in campus life and the academic community. The private Diné College network is available through both wired and wireless terminals, but access is not extended to the public at-large. Special requests for public access will be reviewed on the same basis as the Third Party Access.

Public access to the Diné College wireless network is not allowed. To ensure the continued privacy of the Diné College network, security measures, policies and standards are implemented to only grant access to the network through campus facilities or through authorized user authentication and access codes, such as access passcodes, login accounts and passwords. Devices using the College’s wireless network will be configured by the Diné College ITD support personnel to require the registration of such a wireless device to an authorized Diné College user.

**B. Internet Usage Policy**

Employees are responsible for reading and adhering to the Diné College Personnel, Policies, and Procedures when using the Internet. Violations of certain policies can occur through the use of the Internet. Investigations of violations of those policies can include evidence obtained through the use of the Internet.

If a user of Diné College Internet service is unsure about what constitutes acceptable Internet usage, the user should ask their supervisor or ITD for further guidance and clarification.

**1. Acceptable Use**

- a. Diné College users are expected to use the Internet responsibly and productively. Internet access is not limited to job, school-related activities and to a certain extent personal use is allowed.

- b. Job and school-related activities include business, research and educational tasks that may be found via the Internet that would help in a staff, faculty and student's role.
  - c. Student personal use is allowed to the extent that it does not interfere with business and education and to the extent there is no unauthorized distribution of copyrighted material. Diné College reserves the right to limit or discontinue personal use by blocking streaming and social media sites or other personal use activities if the use impedes business or educational network communication, violates the intellectual property rights of others, or otherwise constitutes unlawful or unauthorized access.
  - d. Employees accessing the Internet with College-owned equipment shall limit their personal use to a minimum and usage should not be performed during business hours.
  - e. All Internet data that is composed, transmitted and/or received by Diné College computer, network, and internet systems is considered to belong to Diné College and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties. Employees have no expectation of privacy of their internet searches, internet browser history, or other data composed, transmitted, and/or received through Dine College computer, network, and internet systems.
  - f. The equipment, services and technology used to access the Internet are the property of Diné College. The College reserves the right to monitor Internet traffic and access data that is composed, sent or received through its online connections.
  - g. All sites and downloads may be monitored and/or blocked by Diné College if they are deemed to be harmful, unlawful, unauthorized, and/or not productive to business.
  - h. The installation of software on any Dine College equipment including, but not limited to, instant messaging software is strictly prohibited.
2. Prohibited use of the Internet by Staff, Faculty and Students includes all harmful, unlawful, or unauthorized use. This includes, but is not limited to:
- a. Streaming radio or music services using College computers in College offices during business hours.
  - b. Unauthorized distribution of copyrighted material.
  - c. Using computers to perpetrate any form of fraud, and/or software, film or music piracy.
  - d. Stealing, using, or disclosing someone else's password without authorization.
  - e. Downloading, copying or pirating software, media files and electronic files that are copyrighted or without authorization.
  - f. Sharing confidential material, trade secrets, or proprietary information outside of the organization.
  - g. Hacking into unauthorized websites.
  - h. Sending or posting information that is defamatory to the college, its products/services, colleagues and/or consumers.

- i. Introducing malicious software onto or jeopardizing the security of the College network and/or systems.
- j. Defeating or attempting to defeat security restrictions on college systems and applications
- k. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- l. Passing off personal views as representing those of Diné College.
- m. Academic cheating and plagiarism.
- n. Accessing any Dine College course materials for which distribution and use has been specifically prohibited by the instructor. This includes, but is not limited to Diné College materials found on crowdsourcing course sites, such as Course Hero, Grade Buddy, and Koofers, which contain materials such as graded quizzes and exams, homework answers, etc., along with any questions that are or might be intended for future quizzes and exams.

### C. Social Media Policy


This policy provides guidance for staff, faculty and student use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information and media with others in a contemporaneous manner.

Social media use should not interfere with employee's or student's responsibilities at Diné College. The primary purpose for Diné College computer systems is to be for business and academic purposes.

The following principles apply to professional use of social media on behalf of Diné College as well as personal use of social media when referencing Diné College.

1. Users should be aware of the effect their actions may have on their and Dine College's reputations. The information that users post or publish may be public information or otherwise accessible for a long time.
2. Users should be aware that Diné College may observe content and information made available by users through social media. Users should use their best judgment in posting material that is either inappropriate or harmful to Diné College, its employees or consumers.
3. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are unlawful, unauthorized, defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile workplace or student community environment.
4. Employees are not to publish, post or release any information that is considered confidential. If there are questions about what is considered confidential or protected by FERPA, employees should check with the Human Resources Department and/or supervisor.

5. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized Diné College External Affairs spokesperson.
6. If users encounter a situation while using social media that threatens to become antagonistic or threatens to harm others or themselves, this should be reported either to IT or supervisory staff. Supervisors and IT must report every incident to Security and their chain of command.
7. Users should get appropriate permission before posting images of current or former employees, board members, vendors or suppliers. Additionally, users shall get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
8. When using Diné College computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Diné College blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is prohibited and could result in disciplinary action.
9. If employees publish content after-hours that involves work or subjects associated with Diné College, a disclaimer should be used, such as this: "The opinions on this site are my own and may not represent Diné College positions, strategies or opinions."
10. It is imperative that employees keep Diné College related social media accounts separate from personal accounts. Use of College email addresses to establish personal social media accounts is strictly prohibited.

 <p style="text-align: center;"><b>Information Technology Policies Manual</b></p>	<b>Section 300.03</b>
	Policy: <b>INFORMATION TECHNOLOGY SECURITY POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: SPECIFIC USE</b>	
Reference:	

Diné College acknowledges the obligation to provide adequate security and protection of all Information Technology (IT) usage within its domain of ownership and control. This policy serves as an umbrella that governs all other Diné College policies pertaining to IT usage on campus, and complies with the appropriate IT policies.

It is also the intent of Diné College to take precautions to prevent revealing specific security policies, standards and practices containing information that may be confidential or private regarding Diné College business.

The Diné College IT security policy is acknowledged as a “dynamic” document that may require alteration periodically to address changes in technology, applications, procedures, legal and social imperatives, and unanticipated changes.

1. Information Technology Security  
It is the sole responsibility of ITD to provide oversight management of all tasks and procedures that directly pertain to maintaining IT security on campus. It is the responsibility of all members of the college community to participate and share this obligation, as specified by all supportive policies and procedures pertaining to technology use on campus.
2. IT security is defined as:
  - a. Protecting the integrity, security, availability and confidentiality of information assets managed by Diné College.
  - b. Protecting information assets from unauthorized release or modification, and from accidental or intentional damage or destruction.
  - c. Protecting technology assets such as hardware, software, telecommunications, networks (infrastructure) from unauthorized use.
3. IT security will be maintained by upholding the following guidelines and standards:
  - a. Diné College will operate in a manner consistent with the goals of the Information Technology Department to maintain a shared, trusted environment within Diné College and within the College community system for the protection of all data relating to business and education.
  - b. Diné College will maintain an IT security audit portfolio that includes comprehensive documentation of all security processes and configuration of all firewalls and defensive mechanisms, such as virus and malware

protection will be included in this audit portfolio. This portfolio and all documentation related to any security policies will be maintained by the Diné College ITD.

- c. Diné College will ensure that all college employees are appropriately familiar with all IT security policies and procedures, and are aware of their personal responsibilities to protect IT resources on campus. Diné College will provide training to each employee in the security procedures for which they are responsible.
- d. Diné College will review its security processes, policies, procedures, and practices annually. In the event of any significant changes to its business, computing, or telecommunications environments, Diné College will make appropriate updates as necessary.
- e. A compliance audit of this IT security policy will be conducted when deemed necessary. The nature and scope of the audit must be commensurate with the extent that Diné College is dependent on secure IT to accomplish its critical business functions. Diné College will maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit.

#### A. Responsibilities

Information Technology Department (ITD):

1. Providing the college with secure business applications, services, infrastructures, and procedures for addressing the business needs of the College.
2. Following and enforcing internal security standards established for creating and maintaining secure sessions for application access.
3. Notifying the appropriate administrator(s) when an individual or individuals have knowingly compromised IT security on campus. ITD is not responsible for determining disciplinary action for individuals who violate IT security policies. This responsibility will be managed by the respective campus office, administrator, or local law enforcement, depending on the scope and nature of the violation.

#### B. Security Breach Notification Procedure

This procedure governs the actions of any Diné College school official who discovers or is notified of a breach or possible breach of the security of unencrypted personal information collected and retained by Diné College as computerized data. This breach can be the result of a compromise of a Diné College computing system or network, the loss or theft of any physical device in which personal information is stored, or the loss or theft of any storage medium upon which personal information is maintained.

If the security of any Diné College system storing or processing computerized data that includes unencrypted personal information is compromised, the owner or licensee of that information must be notified by the College of the breach of the system if the information was or is reasonably believed to have been acquired by an unauthorized person. This disclosure shall be made as quickly as possible following



discovery or notification of the breach. ITD will take any measures to determine the scope of the breach and restore the integrity of the affected data system. A notification may be delayed if law enforcement needs to be contacted for a criminal investigation.

#### 1. Physical Breach

- a. If a report is made to the Diné College Security office of the theft of a computing or storage device, the Security office will:
  - 1) Follow their normal procedures regarding theft of college property;
  - 2) Report it to law enforcement, and act as liaison with any law enforcement agency involved in the situation;
  - 3) Notify ITD of the incident.
- b. If a report is made to ITD of the theft of a computing or storage device, ITD will:
  - 1) Notify the Security office;
  - 2) Provide any inventory information to the supervisor of the theft;
  - 3) Participate in any investigatory actions as directed by HR.


#### 2. Technical Breach

A technical breach is defined as the discovery by technical support staff of a breach of security of a computer or the Diné College network.

- a. If the presenting incident is discovery of a network breach, technical support personnel will:
  - 1) Begin network and computer technical investigations addressing intrusion detection and incident response. This will continue until the security and technical aspects of the situation are resolved.
  - 2) Report to IT Director, all aspects of the breach and how it occurred,
  - 3) Determine if a person or group responsible can be named.
  - 4) Determine safeguards that need to be put in place to prevent a reoccurrence.
  - 5) In some circumstances, it may be appropriate to report a breach of the security of the network or Diné College computers to law enforcement, as well.
  - 6) The IT Director, VP of Administration & Finance and law enforcement will:
    - a) Consult regarding the nature and scope of the security breach and determine whether law enforcement needs to be engaged;
    - b) Decide whether and to what extent members of the Dine College campus community and victims of such breach need to be notified;
    - c) Research each incident and determine how it is to be handled.
  - 7) If it is determined that a breach may have compromised the security, confidentiality, or integrity of Diné College-managed personal information, the Director of Information Technology (or designee) will initiate a meeting as soon as possible with a team consisting of the following or their designees:
    - a) Director of Information Technology

- b) VP of Administration & Finance
- c) Security Supervisor
- d) Director of Enrollment Management (if student data may be involved)
- e) Director of Human Resources (if staff data may be involved)
- f) IT Network security administrator
- g) Technical representatives from ITD, as required

The Director of Information Technology will notify the President of the College that the team has been activated and will provide updates regarding actions taken, as appropriate.

 <p style="text-align: center;"><b>Information Technology Policies Manual</b></p>	<b>Section 300.03A</b>
	Policy: <b>INFORMATION TECHNOLOGY SECURITY PLAN</b>
	Adoption date:
	Effective date:
<b>SUBJECT: SPECIFIC USE</b>	
Reference: GLBA, FERPA	

Pursuant to and in accordance with the Gramm-Leach-Bliley Act, the Information Technology Security plan was developed. This document summarizes the Diné College’s comprehensive written Information Technology (IT) Security Plan mandated by the Federal Trade Commission’s Safeguards Rule and the Gramm-Leach-Bliley Act (GLBA). In particular, this document describes the IT Security Plan elements pursuant to which the Institution intends to:

- 1) Ensure the security and confidentiality of covered records, and
- 2) Protect against any anticipated threats or hazards to the security of such records, and
- 3) Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to the College’s IT consumers.

The IT Security Plan is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including Family Educational Rights and Privacy Act (FERPA).

**A. Designation of Representative:**

The Institution’s IT Operation Manager is designated as the IT Security officer who shall be responsible for coordinating and overseeing the IT Security Plan. The IT Security officer may designate other representatives of the institution to cover and coordinate a particular element of the IT Security Plan.

**B. Scope**

The IT Security Plan applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information:

- 1) A student or other third party provides in order to obtain a financial service from the Institution,
- 2) About a student or other third party resulting from any transaction with the Institution involving a financial service, or
- 3) Otherwise obtained about a student or other third party in connection with providing a financial service to the person.


**C. Elements of the IT Security Plan**

- a. Risk Identification and Assessment: The institution intends, as part of the IT Security Plan, to undertake to identify and assess external and internal risk to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the IT Security Plan, the IT Security Officer will establish procedures for identifying and assessing such risk in each relevant area of the Institution's operation, including:
  - i. Employee training and management: The IT Security Officer will coordinate with representatives in the Institution's Human Resources and Financial Aid offices to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current Personnel, Policies and Procedures Manual and the IT Policy.
  - ii. Information System and Information Processing and Disposal: The IT Security Officer will coordinate with representatives of the Institution's Financial Aid and Business Office to assess the risks to nonpublic financial information associated with the Institution's information system, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution's IT Policy Section 200.02: USE OF THE DINÉ COLLEGE NETWORK AND DATA MANAGEMENT SYSTEMS POLICY. The IT Security Officer will also assess procedures for monitoring potential information security threats associated with software systems and for managing security updates for software and operating systems.
  - iii. Detecting, Preventing and Responding to Attacks: The IT Security Officer will coordinate with other relevant units to evaluate procedures for and methods of detecting, preventing and responding to attacks, other systems failures and network access. The IT Security Officer will evaluate the IT security policies and procedures for coordinating responses to network attacks and developing incident response teams and policies. The IT Security Officer may elect to delegate to a representative of the Department of Information Technology the responsibility for monitoring and disseminating information about known security attacks and other threats to the integrity of networks utilized by the Institution.
- b. Designing and Implementing Safeguards: The risk assessment and analysis shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The IT Security Officer will implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

c. **Overseeing Service Providers:** The IT Security Officer shall institute methods for selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they have access. In addition, the IT Security Officer will work with other designated institutional officials to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.

D. **Adjustment to IT Security Plan**

The IT Security Officer is responsible for evaluating and adjusting the IT Security Plan based on the risk identification and assessment activities undertaken pursuant to the IT Security Plan, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the IT Security Plan.

 <p style="text-align: center;"><b>Information Technology Policies Manual</b></p>	<b>Section 300.04</b>
	Policy: <b>COMPUTER LABS POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: SPECIFIC USE</b>	
Reference:	

Diné College provides students access to computing technology resources in numerous labs and computer classrooms across all campuses. Since the student population on campus is very dynamic and diverse, it is imperative that careful articulation of the policies, expectations, and standards for use of these resources be provided to them, and to the Diné College staff and faculty who support those students in their educational endeavors. This policy is intended to meet that imperative, and to provide all campus users with guidelines for responsible and appropriate use of these campus computing and technology resources.

The primary purpose of the Diné College computer labs is to provide computing technology resources for students and to facilitate the exchange of information related to, and in furtherance of the education, research and academic missions of the College. The goals of the Diné College computer labs are to:

- Provide a computer labs environment across centers that are supportive of learning.
- Help assure the integrity and reliability of the Diné College internal networks, hosts on those networks, and any computing resource connected to them.
- Ensure the security and privacy of the Diné College computer systems and networks.
- Establish appropriate guidelines for the use of Diné College-owned technology.

**A. Prohibited Use**

Using Diné College Information Technology Resources for uses and/or communications that are specifically prohibited in the policy *Use of Diné College Computer Resources Policy*, Section II or which violate any other Diné College policy and/or tribal, state and federal rule or law is strictly forbidden.

Those specifically prohibited uses of any Diné College Information Technology Resource include:

1. Subverting, attempting to subvert, or assisting others to subvert or breach the security of any Diné College network or other Information Technology Resource, or to facilitate unauthorized access.
2. Use of any Diné College Information Technology Resource to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses).
3. Viewing, copying, altering or destroying data, software, documentation, or data communications belonging to Diné College, or to another individual without permission.

4. Individuals allowing another individual (authorized or not to use the Diné College Information Technology Resource) to use their login account password.
5. Disclosing access credentials or masquerading using access granted to another user.
6. Using Diné College computing resources for personal or private financial gain without written authorization.
7. Unauthorized distribution of copyrighted material.

#### B. Access to Computing Labs

Diné College computer labs are open for computer use only by authorized faculty, staff, and currently enrolled Diné College students. Non-student adult visitors may be allowed in monitored labs, including the open lab, to assist or tutor currently enrolled students provided they do not personally use or attempt to use the Information Technology Resources for personal use. In the event of a non-student visitor violating any provisions of this policy or the computer labs procedures, the lab manager for the specific lab may instruct the visitor to leave. Non-student visitors will not be allowed into any unmonitored lab.

Faculty and staff may only use Diné College computer labs in furtherance of their support of the learning objectives of Diné College students. Diné College computer labs will not be used to perform duties or tasks normally performed in the employee's office environment.

Access to any Diné College computing lab is controlled by login and password-secured accounts managed through the Diné College network.

#### C. Labs and Classrooms

Diné College provides different types of computing facilities for use in supporting student learning on campus. These policies apply equally in all these facilities, unless exceptions are otherwise specifically stated. These facilities are: electronic classrooms, computer classrooms, specialized computer labs, and open computer labs.

1. Electronic Classrooms provide multimedia capabilities for instruction from a single, centralized instructor station. These rooms are scheduled for use in the same manner as any other classroom at Diné College following standard Diné College policies and procedures.
2. Computer Classrooms provide hands-on technical instruction in a classroom environment. These labs are only available for use during those times that have been specifically scheduled.
3. Specialized Labs are equipped with specialized hardware and software devoted to supporting the program's unique educational mission. These labs support such varying disciplines as physics, music, math and writing, and are often assigned to students as a part of their regular class work. These labs are staffed by faculty and/or lab assistants who provide additional tutorial assistance within the program's specialty.

- a. Use of these labs are restricted to users taking the specific classes supported by the facility.
4. Open Labs will have a standard software installation containing the general productivity software used on campus.

#### D. Sensitive Materials

All Diné College computer labs are considered shared public places. Users should be aware that some materials accessed on the Internet may be considered controversial, offensive, inappropriate or inaccurate. Diné College asks users, out of consideration for others, to take care not to display, or broadcast in any Diné College-shared public place, any images, sounds, or messages that could create an atmosphere of discomfort, harassment or intimidation for others, and to refrain from transmitting such images, sounds or messages to others using Diné College computing resources.

In some situations, the display or broadcast of such materials is necessary to further a legitimate educational purpose. In these cases, Diné College asks that users be sensitive to the public nature of shared facilities and make arrangements to access these materials in a private environment.

In some situations, the display or broadcast of such materials, if unlawful or otherwise prohibited by this Policy could be grounds for disciplinary action.

#### E. General Lab Rules

##### 1. Prohibited uses

Computing labs will only be used for legitimate academic purposes. Food, drink, smoking, bicycles, skateboards and pets (appropriate guide-animals are exceptions) are not permitted.

##### 2. Noise

All Diné College computer labs are intended to be quiet work and study environments, similar to a library. Users are encouraged to:

- a) Avoid excessive noise, keeping the level of conversational noise at a minimum.
- b) Turn off or set cell phones to vibrate.
- c) Take cell phone conversations outside the lab.
- d) Use headphones any time music is played, either from the computer or from personally-owned devices.

##### 3. Children in labs

Diné College computer labs are learning resources whose primary audience is adults. Children under the age of 16 will not be allowed in any Diné College computer lab unless specific written authorization has been granted by the DIT. The primary exception to this is when they are registered for an event or class.

##### 4. Operating hours

Lab hours will be posted in each lab. All users shall complete their work, including obtaining any printouts, before closing time. Users are not permitted



to stay in the computer lab areas after closing time. Refusal to comply may result in sanctions.

5. Printing

Printers are provided in most Diné College computer labs as a privilege for student use only; faculty and staff should refrain from printing in a lab. Users should exercise discretion in the use of printers in computing labs. Most programs have print preview functions which should be used prior to printing any final document. Print usage on the student network may be actively monitored for abuse. Those users identified as printing excessively will be notified and asked to comply with this policy.

6. Data Storage

Users may not store any files on the hard drives of any lab computers without specific permission from computing services. Faculty may, for a class in which the ability to store files locally is a part of the classroom curriculum, negotiate blanket permission to do this for students enrolled in their class. Users are encouraged to save often and to make frequent backups of their storage media.

7. Bumping

All computers in an open lab are available on a first-come, first-served basis. Users accessing software available on another open computer may be asked by lab assistants to vacate a computer with specialized software required by another user and to move to another computer which provides the software they need. Furthermore, any student using any lab computer for non-educational purposes may be bumped by a lab assistant to allow a student needing the computer for educational purposes access.

8. Lost/stolen property

Diné College cannot be responsible for lost or stolen items left in any lab. Items found in the open lab will be sent to the Security office. Users should label all media with their name for easy identification, if misplaced.

9. Aggressive behavior

Aggressive behavior will not be tolerated in any Diné College computer lab. If necessary, lab assistants will report incidents that cannot be resolved in a quiet, orderly manner to the lab manager and/or to the Security office. Sanctions will apply if issue is escalated.

10. Clean workspaces

For safety reasons, it is important that computer lab users make an effort to keep aisles clear of books and backpacks. Additionally, coats or backpacks should not be placed on computers or on tables which have been provided as workspaces in the labs. Any materials brought into a computer lab should be taken out when the user leaves. After classes held in computer labs, instructors will clean any whiteboard, ensure that students have cleaned their workspaces, and clean up any printing area.

11. Equipment in labs

No equipment in any classroom lab may be moved within the classroom or removed from a lab without permission of the DIT. This includes all computer hardware, including monitors, mice and keyboards and peripheral devices, such as surge protectors, UPS or printers. No user should disconnect any technology

resources from any computer or network connection, nor move any tables upon which computing equipment rests without prior approval. All damaged equipment discovered in any lab should be reported to ITD.

12. Unattended workstation security

Users logged into a computing resource in any Diné College lab who physically leave the workstation they are using will electronically lock the computer, if possible. Under no circumstances will users leave a computer unattended and unlocked for more than fifteen (15) minutes. Users should never leave their workstation unattended without first saving any data upon which they are working.


If a computer in the open lab is left unattended for more than fifteen (15) minutes, lab assistants may log the user off the computer to make it available for other users. Any personal effects in the area of the computer will be moved behind the counter for safekeeping until the owner returns.

13. Hacking

Unauthorized access to accounts, files or data held on Diné College computing systems, or the use of Diné College computing systems and networks to access any other system without authorization is a violation of these policies and potentially a criminal offense. Such unauthorized access is strictly prohibited.

F. Responsibilities

All users of the Diné College computer labs have a responsibility to know, understand, and comply with this policy, to understand their responsibilities, and to meet all the expectations of this and all other Diné College IT security policies and standards. These responsibilities include assumption of any civil and/or criminal liability which may arise from their individual use or misuse of Diné College technology resources.

 <p style="text-align: center;">Information Technology Policies Manual</p>	<b>Section 300.05</b>
	<b>Policy: USE OF DINÉ COLLEGE INFORMATION TECHNOLOGY RESOURCES BY THIRD PARTIES POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: SPECIFIC USE</b>	
Reference:	

Diné College frequently provides access to its Information Technology Resources, including computer facilities, to private company resources, tribal offices and community members to conduct College business when such resources are not in direct use for business or academic purposes, provided such use substantially relates to and does not interfere with the mission of the College. This access to Diné College facilities includes access to the wireless network, computer classrooms, computer labs, and electronic classrooms on campus.

**A. Authority**

The Director of Information Technology has primary responsibility for all aspects of third party access to all Diné College IT resources. These entities must agree to comply with this Policy, the security policies, and standards of Diné College.

Diné College, through ITD administrative representatives, reserves the right to determine, at any time, what constitutes appropriate use of the Diné College technology resources and the Diné College network resources, including any access and/or any computing services provided by Diné College.

**B. Permission for Temporary Use**

Any of these entities must provide documentation of the duration, the list of systems and access required and the location where access is required. This request must be approved by the Director of IT.

ITD personnel will create a Help Desk Ticket to document the access and actions taken during the period of access.


**C. Limitations on Use**

All third party use will have a documented duration which will be reviewed at the end of the duration. Access will need to be renewed with a new approval for the level of access.

**D. Security Rights**

Third Parties are granted standard security privileges or access to the computing equipment in Diné College computer resources sufficient to accomplish their business or educational goals. Individual decisions to allow more access beyond the

standard rights will be made by the ITD. The business impact of the request will be evaluated and balanced against the potential risk and threat to the College network, using the IT security standard addressing security privileges as a guideline.

	<b>Information Technology Policies Manual</b>	<b>Section 400.01</b>
		Policy: <b>SOFTWARE LICENSING COMPLIANCE POLICY</b>
		Adoption date: July 24, 2018
		Effective date: July 24, 2018
<b>SUBJECT: STANDARDS POLICY</b>		
Reference:		

Diné College acquires software licenses for the use and distribution to faculty, staff and students for productivity and efficiency of the operation of the college and its interaction with the students. Diné College expects all students, faculty, and staff members to comply with applicable local, state, and federal laws governing licensed software. This policy ensures that Diné College and all its employees and students follow the letter and spirit of both state and federal law regarding software licensing.

**A. Software Licensure**

Diné College acquires software licenses, and must use the software and documentation only in accordance with applicable license agreements. The College does not own such software or its related documentation. Except as specifically authorized by a software licensor in an agreement, faculty, staff, and students are prohibited from reproducing licensed software or related documentation. It is the responsibility of software users to be aware of limitations on use and reproduction described in the license agreement related to specific software and to use licensed software strictly in accordance with such limitations. A copy of the software license agreement should be kept with the software for easy reference to determine if copies can be made, e.g., for backup or archival purposes, and to assure compliance with all provisions of the software agreement. If a College department purchases software outside of the standard for Diné College, it is responsible for licensing, compliance, maintenance and service for the software.

College faculty, staff, or students making, acquiring or using unauthorized copies of licensed software or related documentation, or otherwise misusing licensed software may be disciplined as appropriate. The individual may subject the College to and also be subject to exorbitant civil damages and criminal penalties including fines and imprisonment.

**B. Authority**

This policy is intended to be in compliance with current software licensing laws. None of those stipulations are replaced by this policy, which is intended to augment the provisions articulated there.

These licensing laws and policies govern the purchase, lease, license and use of computer software, audio and video recordings, printed matter and data captured in various other media.

### C. Permission

The College may enter into written agreements with software licensors which detail the rights and limitations regarding the appropriate use of the software.

Faculty and staff members with questions about the interpretation of license agreements may contact the Director of Information Technology.

### D. Prohibited Use

It is prohibited to copy, reproduce, or transmit software on Diné College computing equipment, except as allowed by this policy or permitted by the software license. It is also prohibited to install, or cause to be installed, on any Diné College computing equipment, software for which legitimate verification of ownership cannot be documented. Furthermore, any unlawfully obtained software is prohibited from being installed on any Diné College computing equipment.

### E. Ownership

Diné College is the sole owner of all software purchased using tribal, state or federal funds or grants where Diné College is the fiscal agent. The Director of Information Technology or his/her authorized designee is authorized to sign license agreements on behalf of the College.

Diné College retains ownership of all data and/or software created or modified by its employees as a part of their regularly assigned job duties. *See Dine College Intellectual Property Rights: Personnel, Policies and Procedures Manual.* Programs written by Diné College employees on personal home computers for their own use are not covered by this policy. Exemptions would need to be negotiated by the employee through the Vice President of Administration and Finance prior to the start of any data or applications development.

### F. Violation Indemnification

Diné College reserves the right to refuse to defend or indemnify any faculty member, student or staff member named in a lawsuit arising from alleged licensing infringement activity, and to refuse to pay any damages awarded by a court of law against such person if the violation resulted from willful violations or negligence. Any fines assessed to the College because of the illegal use of software by an individual will be passed on to the user responsible for the misuse.


### G. Responsibilities

#### 1. Institutional Responsibility

- a. Diné College has vested in ITD the primary responsibility for establishing the procedures and processes to ensure that the use of software on the campuses comply with the law. These responsibilities include:

- 1) Monitoring compliance with this policy and all related expectations;

- 2) Preparing inventories of Diné College-owned software installed on computers for use in work-related activities both on and off-campus;
  - 3) Maintaining inventories and documentation related to the lawful use of individually-owned software on Diné College-owned computers;
  - 4) Establishing and maintaining a centralized software and license repository;
  - 5) Assisting Diné College and its technology users in obtaining and documenting that software which may legally be used;
  - 6) Developing and maintaining adequate record-keeping systems.
- b. Diné College has also established ITD to manage all aspects of Information Technology Resources security on campuses. With regards to software licensing compliance, the Diné College ITD will ensure that:
- 1) Only authorized software is acquired and used on Diné College computers;
  - 2) Diné College has adequate policies, procedures, and practices to insure compliance with its licensing;
  - 3) In carrying out these responsibilities, Diné College ITD conducts periodic internal software audit on campuses in addition to actively monitoring and scanning of Diné College systems.
  - 4) Diné College ITD will actively cooperate and share information with appropriate agency in investigations into alleged violation of the licensing law.
2. Employee Responsibility
- a. Employees shall comply with the terms and conditions of all licensing agreements. Employees have an individual responsibility for familiarizing themselves with their obligations under this policy and for understanding the license obligations related to software they are using.
  - b. Diné College Information Technology Resources authorized for off-site use by an employee for official purposes are subject to the same expectations of licensing compliance as would be applicable if the employee were located in a Diné College facility or other official duty station. No employee will use unauthorized copies of software on Diné College-owned computers regardless of where they are located.

 <p style="text-align: center;">Information Technology Policies Manual</p>	<b>Section 400.02</b>
	Policy: <b>TECHNOLOGY HARDWARE AND SOFTWARE ACQUISITION POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: STANDARDS POLICY</b>	
Reference:	

A. Purpose

The purpose of this policy is to provide guidelines and the process for acquiring and maintaining institution-wide hardware, software and cloud services identified as mission critical. The intent of the policy is to ensure that computer technology and services comply with College defined support standards and security safeguards.

B. Responsibilities

Enterprise network, server and storage appliances for institutional-wide applications will be acquired by the Information Technology Department. The Network Operating Center, ITD server rooms and closets are specially designed with the environment conducive to equipment efficiency and with backup power.

ITD is responsible for the system management, updates, upgrades and new releases. These systems will be managed and maintained regularly to assure all maintenance procedures are properly scheduled. Planning of such processes will be coordinated with all users impacted.


ITD is responsible for all back-up and restore procedures. All systems will be backed up regularly and with efficiency for restore times.

Here are the requirements when acquiring this type of equipment.

1. All computer technology for business and academics must be purchased through ITD.
2. All computer technology assets purchased with College funds are the property of the College and not a specific faculty or staff member's department property. College funds include, but are not limited to, grant funds, restricted, or unrestricted funds.
3. Funding for maintenance or support agreements must be coordinated with ITD prior to purchase.
4. ITD must approve any server or specialized appliance requiring network connectivity prior to acquisition. In addition, the device must meet the required conditions for connectivity.
5. Network connected servers or appliance devices must reside in an environment managed by ITD must approve any technology that incorporates any kind of wireless access to ensure meeting DC guidelines and standards prior to purchase.



6. ITD must review and approve any software application system or cloud service prior to acquisition.

 <p style="text-align: center;">Information Technology Policies Manual</p>	<b>Section 400.03</b>
	Policy: <b>TECHNOLOGY HARDWARE AND SOFTWARE REPLACEMENT AND UPGRADE POLICY</b>
	Adoption date: July 24, 2018
	Effective date: July 24, 2018
<b>SUBJECT: STANDARDS POLICY</b>	
Reference:	

A. Purpose

This document defines Diné College’s policy regarding the replacements of all college-owned technology equipment at the end of its life cycle and also the upgrades of institution-wide software. Adequate computer and network hardware and software are essential for the delivery of instructions, student learning, research and creative activities; and for the efficient and effective management of the institution. Rapid changes in technology require that a well-managed institution have a systematic plan for upgrading and replacing technology to ensure that it offers access to the most basic services.

The purpose for this plan is to:

1. Provide consistency of hardware and maintain a standard that will limit the variety of parts and supplies.
2. Regulate the purchasing of computers by establishing a useful life table.
3. Improve the level of support by limiting the number of operating systems, office productivity products and other standard software installed in these systems.
4. Reduce the downtime and outages because of outdated or incompatible equipment.
5. Provide a guideline for evaluation or assessment of IT infrastructure on a regular basis
  - a. To assess bandwidth usage and the need to expand or enhance capabilities
  - b. To reduce possible failures due to normal aging.
  - c. To assure sustainability by replacing it with newer technology.
6. Provide sufficient backup solutions for power, network equipment and server systems for redundancy and high availability.
7. To preemptively implement necessary changes.

This systematic plan is meant to align with the College’s Strategic Plan and to provide a framework for meeting the technology needs of the stakeholders of Diné College. Input from the Technology Committee, the Director of IT, the Distance Learning Coordinator, Dean, Vice President of Student Success and the Vice President of Administration and Finance could help encapsulate varying ideas for a more complete plan.

**B. Responsibilities**

1. Administration/Department Heads - Each department head is responsible for identifying any exception (earlier or delayed replacements/upgrades) necessary to ensure that an employee can effectively perform his/her job duties. This information is then passed on to ITD for the replacement or upgrade process. The VP of Administration and Finance is responsible for reviewing and approving requested exceptions and divisional budgets.
2. ITD - ITD is responsible for acquiring estimates for replacements and upgrades and also executing equipment replacements institution-wide including software upgrades according to established replacement cycle. ITD also makes technical decisions on equipment and software standards and upgrades and replacements based on industry trends, software development life cycles, costs and risks to systems stability.

**C. Plan Statement**

Diné College will maintain modern computer and network hardware and software capable of supporting its educational and business activities. To accomplish this, technology hardware will have to be budgeted for replacement through the appropriate department budget and replaced and upgraded according to the schedule below:

<b>Category</b>	<b>Description</b>	<b>Replacement Time frame</b>
High-performance Servers	This category encompasses all high-performance and high-use servers. These servers perform mission critical activities and/or provide access to critical services on a daily basis.	Fiscal year immediately after 3 <sup>rd</sup> - 5 <sup>th</sup> year of use
Laptop and Apple Computers  Includes tablets valued over limit of expensed equipment.	This category encompasses all laptops, Apple system, iPads and high-valued tablets includes all associated docking stations and monitors as a single unit.	Fiscal year immediately after 3 <sup>rd</sup> - 4 <sup>th</sup> year of use
Desktop/Workstation Computers	This category encompasses all desktop computer systems and includes the CPU and monitor as a single combined unit.	Fiscal year immediately after 5 <sup>th</sup> year of use
General Use Servers	This category encompasses all servers not classified as "high-performance". These	Fiscal year immediately after 5 <sup>th</sup> year of use

	servers provide mission-essential services and perform activities supporting the academic, service and business goals of the institution.	
Network Hardware	Network hardware includes repeaters, routers, switches, bridges, access points and other communication devices.	Fiscal year immediately after 5 <sup>th</sup> year of use
Desktop Peripherals	Desktop peripherals include printers, scanners, projectors, and interactive whiteboards (if applicable).	Fiscal year immediately after 7 <sup>th</sup> year of use
Cable Plant and Physical Infrastructure	The copper and fiber optic wires that connect data/information stations together and comprise the network infrastructure.	Fiscal year immediately after 10 <sup>th</sup> year of use
Server Room Air Conditioner	Cooling system for the server room	Fiscal year immediately after 7 <sup>th</sup> - 10 <sup>th</sup> year of use
UPS	Uninterruptible Power Supply unit to sustain business from abrupt shutdown in the event of sudden power outage	Fiscal year immediately after 7 <sup>th</sup> - 10 <sup>th</sup> year of use
UPS Batteries	Batteries/power source for UPS	Fiscal year immediately after 3 <sup>rd</sup> - 4 <sup>th</sup> year of use
Printers	Printer comes with built-in double-sided duplex printing capability and a 1-year warranty (extended warranties may be purchased). Choices include black and white, color, and multifunction printing.	Printers will be replaced when deemed necessary and when frequency of repairs exceeds frequency of use. Replacement will be determined by individual department and ITD based on repair records and age of the printer.
Tablets (expensed)	Tablets not in the laptop category	As useful life dictates, 2-3 years and as expense budget allows.

If a hardware item is determined to be irreparable by ITD or if the cost to repair exceeds the current market value of the item, the item may be replaced earlier than indicated in the table above with all costs for replacement covered by the College responsible department budget.

If a department elects to replace an item earlier than the identified replacement cycle, both the budget officer and VP over the reporting line must approve the request and the electing department assumes all costs for replacing the item.


#### D. Software Upgrades

Related to software, all systems should be running the current version or most recent prior version of manufacturer-released software packages. If a college-owned system is found to be running an older version (current -2 or older) of any institution-wide software package (Operating System, office productivity suite, or other site-licensed desktop application), it will be upgraded to the most recent version as soon as possible.

#### E. Replacement Requirements

All replacements will adhere to a single standard for each equipment type. Departments must surrender a like device (computer, peripheral, etc.) for each device replaced. Departments may not repurpose existing devices to expand the number of technology devices supported. All enhancements to or changes from the standard resulting in a cost-higher than that of the standard will be charged to the requesting department's budget.

If a department keeps or maintains any special-purpose software or peripherals, they must be compatible with the new equipment and all institution-wide software packages. Otherwise, the department is required to purchase the software or peripheral upgrade.

	<b>Information Technology Policies Manual</b>	<b>Section 400.04</b>
		Policy: <b>PRINTER STANDARDIZATION POLICY</b>
		Adoption date: July 24, 2018
		Effective date: July 24, 2018
<b>SUBJECT: STANDARDS POLICY</b>		
Reference:		

ITD and Diné College Purchasing will standardize on a network printer from a vendor using special government rate pricing for administrative and institutional use at the College. Each printer will come with built-in double-sided duplex printing capability and a 1-year warranty. Extended warranties can also be purchased with proper justification. Choices will include black and white, color, and multifunction printing. Standardization will provide for better College discounts and support.

It will also enable us to keep our printing services sustainable. Approved printer model has undergone reviews and testing to confirm its usability, functionality and supportability on the ITD network print queue system, and will be made easily accessible on managed computers.

Purchase of the recommended printers will ensure a quick and smooth installation. In the event you feel you have printing needs not addressed by the recommended model, please contact the ITD or submit a Help Desk Ticket before purchasing a non-recommended printer model. IT personnel will help you find a printer which will meet your needs and also supportable on IT networks. All printers already connected to the Diné College networks and print server will continue to be supported.

## **Appendix A – Definitions**

All terms defined in Diné College policies are applicable.

### **Diné College Network**

This includes the administrative and student local area networks (LAN), the wide area networks (WAN) supporting sites separated from the main Diné College campus, Internet connectivity, networked infrastructure devices such as hubs, switches and servers, warrior web, and all other computers, networks and electronic messaging systems operated for the benefit of Diné College employees and students.

### **Diné College Data Management Systems**

This includes the student information management system, human resources system, finance information management system, cashiering, degree audit and individual databases created by individual departments or the college.

### **Diné College Information Technology Resources**

Includes, but is not limited to, Diné College-owned desktop, laptop or macs or servers, hardware or software; software licenses; workstations; data systems; personal digital assistants; electronic messaging systems; e-mail systems; telephones—both wired and cellular; SCAN services; voice mail systems; fax machines; Diné College network resources, whether wire-based or wireless; Internet connections, accounts or access; and documentation photocopiers authorized by Diné College to be used by employees, students and/or other campus users.

### **Disclosure**

This occurs when an unauthorized user gains access to information. Disclosure often occurs when messages are forwarded to unauthorized users.

### **Help Desk Ticket**

A form from the Warrior Web site can be accessed to submit a request for assistance for any issue for College owned computer equipment. It can be issued for outages, errors, incorrect results or access issues. It can also be open to request any technology hardware or software. All Help Desk Tickets will be assigned to a technician or administrator that has authority and capability to handle your request.

### **Masquerading**

This is when a user presents self to the system as another user. This may be done in order to gain unauthorized access to information or resources, to disseminate (mis)information in another's name, or to block or deny a system from operating correctly.

### **Off-site**

Locations away from Diné College campus or Dine College properties or centers.

### Unauthorized Access

Includes gaining access to accounts, resources, messages or files to which one is not granted privilege by the owner or sender.

### Lab assistants

These are individuals, maybe students, assigned to particular labs whose purpose is to facilitate the general use of the lab. They are usually familiar with the equipment and software in that lab hence enabling them to provide users with assistance. They are also versed in Diné College policies and procedures which apply to that lab, and may have rudimentary technical troubleshooting skills. They refer technical problems in labs to the Diné College support technicians. Lab Assistants are not able, nor authorized to perform software installations or equipment repair without direct supervision from support technicians, or the director of computing services.

### Support technicians

These are full or part-time employees of the college able and authorized to fully support all equipment in the computer labs.

### Software

Software is a generic term for organized collections of computer data and instructions, often broken into two major categories: system software that provides the basic non-task-specific functions of the computer, and application software which is used by users to accomplish specific tasks. Unless otherwise stated, "software" includes all freeware, shareware, and third-party products, as well as commercially acquired products.

### Copying

For purposes of computer software, copying includes loading the software into the random access memory (RAM) when the computer is booted up, downloading software from an Internet website, creating a duplicate of any medium upon which software is stored, saving software from its original media onto the hard drive of a computing system, or any other potentially permanent duplication.

### Electronic Messaging Systems

Include, but are not limited to, electronic mail systems, such as E-mail that store and transmit communications; voice mail systems which store and transmit communications; facsimile and imaging equipment that store and transmit images; instant messaging (chat) systems that transmit communications and all similar systems.

### Internet

Includes, but is not limited to, the connection to and the use of interconnected networks in public and private domains to access the World Wide Web, e-mail, file transfer protocols, and other network resources.



**Appendix B – IT Policy Agreement**

**Page intentionally left blank**



**Information Technology Department**

***Computers and Networking to support Teaching, Learning, and Administration***

### **Diné College IT User Agreement**

I have read, understand, and will abide by the above IT Policy when using computer and other Diné College Information Technology Resources owned, leased, or operated by the Diné College. I further understand that any violation of the regulations above is against Diné College policy, unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated.

\_\_\_\_\_  
User Name (please print)

\_\_\_\_\_  
User Signature

\_\_\_\_\_  
Date