IT POLICY

PRANANATH COLLEGE (AUTONOMOUS), KHORDHA

Principal
Pranananth College (Autonomous),
Khordha

Principal
PRANANATH COLLEGE
(Autonomous)
KHORDHA

IT Policy Draft Committee

1.	PRINCIPAL	Chairman
3.	System I/C	Member
4.	Accounts Bursar	Member
5.	Administrative Bursar	Member
6.	Expert from ST dept.	Member
7.	Internet & IT asset	Member

“The NEP 2020 aims at promoting online education consequent to the recent rise in epidemics and pandemics to ensure preparedness with alternative modes of quality education whenever and wherever traditional and in-person modes of education are not possible, has been covered. A dedicated unit to orchestrate the building of digital infrastructure, digital content and capacity building will be created in MHRD to look after the e-education needs of both school and higher education.”

Preamble

The IT Policy aims to promote and regulate digital infrastructure, digital content and online activities within the College with an emphasis on safe and responsible use of information and communication technology. In the light of National Education Policy(NEP)and following recent epidemic situations, the policy document addresses e-education needs and ensures preparedness for implementation of hybrid mode of learning.

1. Introduction

Prananath College (Autonomous), Khordha have its own IT Policy that works as guidelines for using the college IT Infrastructure including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called “Information Technology (IT)”. Hence, this document makes an attempt to propose some IT policies and guidelines that would be relevant in the context of this College

IT policies and related standards apply to all users across the entire Prananath College (Autonomous), Khordha and on campus visitors. This policy apply whether the College's information resources are accessed on- or off-campus.

This policy covers the appropriate use of all IT resources including hardware, software, systems, networks, procurement and maintenance, information security and the information contained therein.

The purpose of this policy is to define rules and requirements for connecting to College networks and systems from any host. These rules and requirements are designed to minimize the potential exposure to students, faculty, employees, vendors, contractors, guests etc.

Internal systems, and fines or other financial liabilities that could be incurred because of those losses. Also, it provides a security framework that will ensure the protection of College Information from un authorized access, loss or damage while supporting the open, information- sharing needs of our academic culture. College Information may be verbal, digital, and/or hard copy, individually-controlled or shared, stand-Alone worked, used for administration, research, teaching, or other purposes.

Further, due to the dynamic nature of Information Technology, Information security in general and therefore policies that govern information security processes are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

The policy applies to all the members of the College and others who handle College managed information including faculty, staff, student, contractors, consultants and visitors of the College The College abide "The Digital Personal Data Protection Act, 2023.

Purpose and Scope of IT Policy:

PNC Provide IT resources to its end-user to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas ofwork.Theseresourceshelpofficialstoremainwellinformedandcarryouttheirfunctionsin an efficient and effective manner.

For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

Misuse of the seresourcescanresultinunwantedriskandliabilitiesfortheCollege.Itis, therefore, expecte dthattheseresourcesareusedprimarilyforCollegerelatedpurposesandin a lawful and ethical way.

Scope:

This policy governs the usage of IT resources from an end user perspective.

This policy is applicable to all the end users of the college.

Objective:

The objective of this policy is to ensure proper access to and usage of IT infrastructure and assets of college and prevent to use by the mis users. Use of resources provided by the Government of India implies the user's agreement to be governed by this policy.

Access to the Network (InternetandIntranet):

a. Ausershouldregistertheclientsystemandobtainonetimeapproval/permission from the Technical Cell before connecting the client system to the college network.

b. Usersshouldnotundertakeanyactivitythroughanywebsiteorapplicationsto bypassfiltering/Policy/Firewall/UTMofthenetworkorperformanyotherunlawful acts which may affect the network's performance or security

c. Users are not allowed to change the NIC configuration, IP address or any other parameters set for accessing College's LAN & WAN without permission of the Technical Cell.

d. Users shall not connect any other devices to access Internet/any other network in the same client system configured for connecting to LAN/WAN of the College without permission.

e. It is the responsibility of the user to ensure that the client system is free from any Virus/Malware/Potential threat softwares/pirated copy of softwares before connecting to the College's network.

Access to the College Wifi network:

For connecting to a College wifi network, user should ensure the following:

a. A user should register the access device and obtain one time approval/permission from the Technical Cell before connecting the access device to the College wifi network.

b. Wireless client systems and wireless devices should not be allowed to connect to the College wireless access points without due authentication.

c. To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

Filtering and blocking of Sites:

a. Technical Cell may block content over the Internet which is in contravention of the relevant provisions of the government Laws and other applicable laws or which may pose a security threat to the network.

b. Technical Cell may also block content, which, in the opinion of the College, is inappropriate or may adversely affect the network security and productivity of the users/organization.

Approving Authority:

1. GB
2. Finance Committee
3. Principal

Technical Cell (System and IT I/C

Applicability:

Applies to all College students, faculty and staff, and all others using computer and communication technologies, including the College's network, whether personally or College owned, which access, transmit or store College or student formation. This policy alsoappliestoallotherindividualsandentitiesgranteduseofCollegeInformation,including, but not limited to, contractors, temporary employees, and others as identified by College

Stakeholders on campus or off campus

✓Students: UG,/PG,/ Research

✓Employees (Permanent/Temporary/Contractual)

✓ Faculty(Permanent/Temporary/Contractual)

✓Administrative Staff(Non-Technical/Technical)

✓Higher Authorities and Officers

✓Guests

Resources

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Desktop/Laptop server computing facility
- Software
- Documentation facility(Printers/Scanners)
- Multimedia Contents

2. Installation Policy

IT Hardware Installation

College network user community need to observe certain precautions while getting their computersorperipheralsinstalledsothathe/shemayfaceminimuminconveniencedueto interruption of services due to hardware failures.

Who is the Primary User?

ComputerSystemissuedindividual(Administrativeofficers/Faculty/staff/research scholar), that individual will be responsible for that system.

· Thosesystemsinthelab/office,departmentHeadshouldmakeanarrangementand make aperson (lab coordinator) responsible for compliance.

B. What are End User Computer Systems?

Computers systems, if any, that are acting as servers which provide services to other user son the Intranet/Internet though registered with the Technical Cell, are still considered under this policy as "end-users" computers.

C. Warranty and Annual Maintenance Contract

Any IT equipment purchased by the College and provided to primary users will be maintained under annual maintenance contract.

Computerspurchasedbyany Section/Department/Projectshouldpreferablybewith3- year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract .The above said maintenance will be under the supervision of the Technical Cell.

D. Power Connection to Computers and Peripherals

· All the computers and peripherals should be connected to the electrical point strictly through online UPS. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.

· All the power connection related issues/ installation of ups/earthing/wiring related issues will be dealt with by the IT Section of college.

E. Shifting Computer from One Location to another

Computer systems may be moved from one location to another with prior written intimation to the IT Cell maintains the record of computer identification names and MAC address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (from the list maintained by Technical Cell is found for any computer system, network connection would be disabled and the same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs the Technical Cell in writing/by email, connection will be restored.

F. Noncompliance

Collegefaculty,staff,andstudentsnotcomplyingwiththiscomputerhardwareinstallation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computers resulting in loss of productivity.Anindividual'snon-compliantcomputercanhavesignificant,adverse effects on other individuals, groups, departments, or even the whole College Hence it is critical to bring all computers into compliance as soon as they are recognized not to be non-compliant.Software Installation and Licensing

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws, College IT policy does not allow any unauthorized software installation on the College owned computers and the computers connected to the College campus network. In case of any such instances, the College will hold the department/individualpersonallyresponsibleforanyunauthorizedsoftwareinstalledonthe computers located in their department/individual’s rooms.

Operating System and its Updating

1. IndividualusersshouldmakesurethatrespectivecomputersystemshavetheirOS updated of their service packs/patches, through the Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. College as a policy encourages the user community to go for open source software such as Linux, Open office etc..to be used on their systems wherever possible.

B. Antivirus Software and its updating

1. Computer systems used in the College have anti-virus software installed, and active at all times. The primary user of a computer system is responsibleforkeepingthecomputersystemsafefromVirus,Malware,Trojanetc.

2. He/sheshouldmakesurethatthesoftwareisrunningcorrectly.Itmaybenotedthat any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use.

3. If these responsibilities appear beyond the end user's technical skills, the end-user is

responsible for seeking assistance from Technical Cell or any service-providing agency.

4. Do not remove or disable anti-virus software.

5. Do not use unauthorized/not licensing Antivirus Solution.

6. Centralized or network based antivirus shall be installed.

C. Back ups of Data

1. Individualusersareresponsibletoperformregularbackupsoftheirvitaldata.Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible and the loss of data is the sole responsibility of the individual.

2. Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned in at least two volumes typically C and D. OS and other software should be on C drive and user’s data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only C drive volume will protect the data loss. However, it is not a foolproof solution. Apart from this ,users should keep their valuable data either on portable hard disks or other reliable storage devices.

Network Device Connectivity and Installation:

Network connectivity provided through the College, referred to hereafter as "the Network", either through an authenticated network access connection, a Virtual Private Network (VPN) connection, or Wireless Connection is governed under the College IT Policy.

IP Address Allocation:

✓ Any computer (PC/laptop/Server) that will be connected to the College network should have an IP address assigned by the IT Cell .Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. Further, each network portion the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

✓ Any IP base device like network printer, smart TV, biometric machine, CCTV/DVR, IP Camera, Video conferencing device, IP Phone etc. is to be installed at any location ,then the concern user should contact IT Cell and get proper IP Address.

✓ Anycomputer(PC/Server)thatwillbeconnectedtotheCollegenetworkshouldhavean IP address assigned by the IT Cell

✓ All network devices should be IPV6 compliant and should support IPV4 till the time all networks and applications are not completely migrated to IPV6.

✓ Following a systematic approach, the range of IP addresses that will be allocated toeach department/section/hosteletc.isdecided.So,anycomputerconnectedtothenetworkfrom that building will be allocated IP address only from that Address pool.

A. Local Area Networks:

✓This policy applies, in it entirety, to School, department, or division Local area networks. In addition to the requirements of this policy, schools, departments, or divisions must register each wireless access point with IT Cell including Point of Contact information. IT Cell Will be responsible for creating wireless access points.

- ✓ School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.
- ✓Ifindividualdepartments/schoolsetc..wantstohaveaninter-buildingwirelessnetwork, prior to installation of such network, it should obtain permission from the College authorities.

B. Structured Cabling as a part of New Buildings:

- ✓ All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan.
- ✓ Engineering Cell/Section may make provisions in their designs for network points/access points in each room and in the corridors based on the input provided by IT Cell or in coordination with IT Cell . All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

Use of Secure Passwords

All users accessing the e-mail services must use strong passwords for security of their email accounts.

Privacy

Users should ensure that emails are kept confidential. Technical Cell shall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone. However, it must be kept in mind that emails are not fully secure and care should be taken when typing email addresses to ensure that it reaches the intended recipient. Moreover, it is also possible that the origin of an email is not what it appears to be and users should not disclose sensitive information such as passwords/any financial information in emails.

Responsibilities of Department/Cell/Section: Policy Compliance

a) All Department/Cell/Section shall implement appropriate controls to ensure compliance with the e-mail policy by their users. Technical Cell shall give the requisite support in this regard.

b) TheDepartment/Cell/Sectionshallensurethatofficialemailaccountsofallits users are created only on the e-mail server of the College

c) Head of Department (HoD) of the department/cell/ section/ unit shall ensure resolution of all incidents related to the security aspects of the e-mail policy. Technical Cell shall give the requisite support in this regard.

d) HoDshallensurethattrainingandawarenessprogramsone-mailsecurityare organized at regular intervals. The Technical Cell shall provide the required support.

Policy Dissemination

a) Head of Department (HoD) of the concerned Department/Cell/Section should ensure dissemination of the e-mail policy.

b) Orientation programs for new teaching, non teaching staff, researchers etc shall include a session on the e-mail policy.

Responsibilities of Users:

Appropriate Use of E-mail Service

a) E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name-based ids can be used for both official and personal communication.

b) Forpersonalcommunication,reasonableuseoftheemailserviceispermitted provided it is not:

i. Of commercial/profit-making nature or used for personal financial gains.

ii. In conflict with College rules, regulations, policies, and procedures; including the email policy.

iii. In conflict with the end-user obligations towards the College as

employer.

c) Bulk emails (including reply-all to such bulk emails) with multiple intended recipients (viz., faculty/ staff/ students) shall be routed through/ upon approval from, the office of the Registrar or the concerned head/ chairperson of the department/cell/section unit or committee.

d) Examples of in appropriate use of the email service

i. Unauthorizedexchangeofproprietaryinformationoranyotherprivileged, confidentialorsensitiveinformation,includingemailIDsand/orpasswords.

ii. Un authorized access of the services. This includes the distribution of emails anonymously, use of other officers' user ids or using a false identity.

iii. Creation and exchange of information in violation of any laws.

iv. Use or attempt to use the accounts of others without their permission.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policyandmayresultindeactivationoftheaccountafterconsultationwiththeCompetent Authority. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

User’s Role

a) TheUserisresponsibleforanydata/e-mailthatistransmittedusingtheCollege e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b) Sharing of passwords is prohibited.

c) The user’s responsibility shall extend to the following:

i) Users shall be responsible for the activities carried out on their clients ystems,

Using the accounts assigned to them.

ii) The reply all' and the use of' distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

iii) Backupofimportantfilesshallbetakenbytheuseratregularintervals.The Technical Cell shall not restore the data lost due to the user's actions.

iv) Users should not open attachments in emails received from unsolicited/un trusted sources unless the attachment has been scanned for viruses.

d) The College may define and implements to rage quotas for both end-user as well as student email accounts. Users are responsible for regular deletion of email which is not of use in order to saves to rage space. Users will be notified via email when they are approaching then do their storage limit. Once the storage limitis exhausted, one final email will be sent to the user, notifying them to reduce the storage below the sanctioned limit. After exhaustion of the storage limit, users will not receive any further email suntil the storage is reduced below the storage limit.

Deactivation:

In case of threat to the security of the College service, the e-mail id being used to impact the service may be suspended or deactivated immediately by the Technical Cell.
Subsequent to deactivation, the concerned user and the competent authority of that respective Department/Cell/Section shall be informed.

Exemption:

Departments/centers operating Intranet mail servers with air-gap are exempted from this policy.

Audit of E-mail Services:

The security audit of G-Suite email services and other departments maintaining their own mail server shall be conducted periodically by an outsourced agency as approved by the Technical Cell.

E-mail account and resultant record:

All the E-mail ids provided to the individual members of academic and administrative community, including the E-mail ids provided to different Branches, Sections, Divisions and Research Centres are supposed to transact the official business through these email ids.

Review:

Future changes in this Policy, as deemed necessary, shall be made by Technical Cell with there commendation of IT Committee and approval of the competent authority.Theabovelaiddown policies particularly 1 to 12 are broadly applicable even to the email services that are providedbyothersourcessuchasgmail.com,rediffmail.com,Hotmail.com,Yahoo.cometc., as long as they are being used from the College's campus network, or by using the resources provided by the College to the individual for official use even from outside.

3. Network/Server Usage Policy and Guideline:

Individual/Stakeholders Responsibility

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities ,or derogatory remarks in communications.

- Access, download, send or receive any data (including images),which (COLLEGE)considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to(college),alter any in formational bout it, or express any opinion about(college),unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email on behalf of(college)unless authorized to do so.
- In any way in fringe any copyright, database rights, trademarks or other intellectual property.
- Care must be taken to not leave confidential material on printers or photocopiers.· Violate the IT ACT of GOI provided from time to time.

Guide lines for Desktop/PC/Laptop etc Users:

The Guidelines are meant for all members of COLLEGE Network User Community and users of College Network. Due to the increase in hacker activity, College IT Policy has put together recommendations to strengthen system security.

The following recommendations include:

i. All desktop computers should have the latest version of antivirus.

ii. When a desktop computer is installed, all operating system updates should be applied.

iii. All Windows desktops should have an administrator account that is not used as the regular login account.

iv. The password should be difficult to break. Suggested to mix upper case, lower case, or other characters not easily found in a dictionary, and make sure they are at least eight characters long. Also suggested to change the password on regular interval time

v. Don' to penne mail or attachments from unknown sources.

vi. The guest account should be disabled.

vii. Disconnect from the Internet when not in use.

viii. When the hard disk of the PC is form attend, the OS and all the application software should be installed from the original CD soft he soft ware. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

ix. IT Cell recommends a regular back up strategy. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine. Departments should arrange/purchased at a storage devices as part of the requirement from the department. If the user feels he/she can store data on Cloud etc.

x. Do not allow anyone else to use their user ID and password on any(college)IT system

xi. Do not leave their user accounts logged in at an unattended and unlocked computer.

xii. Use someone else's user ID and password to access(college's) IT systems. Do not leave the password unprotected (for example writing it down).

xiii. Documents that are no longer required to be shared will be removed from the shared folder.

xiv. All shared folders should be password protected.

xv. Remote Login should be disabled and only in special cases it would be permitted with permission of IT Cell (In charge).

xvi. End user will be solely responsible for use/installation of any unauthorized/restricted software.

Data Backup, Security, and Disclaimer

IT Cell will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an IT Cell staff member in the process of helping the user in resolving their network/computer related problems.

Users may note that the College's Network Security System may maintain a history of in fractions, for each user account. Incase of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate College authorities.

Wi-Fi implementation and usage

Wi-Fi Access and locations

1. Wi-Fi Access Point: Wi-Fi facilities may be made available at canteen, library, hostels, department/ cell/section, laboratories, guesthouse and officers residences etc. The decision of IT Cell will be final to decide the location of such access points.
2. Wi-Fi Access Points: may be placed temporarily on demand in auditorium and other places, for conference, workshops, symposia and any other important events.
3. Inspecialcasestheindividualordepartmentmayapproachthetechnicalcelltoget propersecureconfigurationandregistrationofthepersonal/department'sAccess Points or routers with proper approval of the concerned head.

Methods for Wi-Fi users Authentication/ Authorization and Activity Logs

1. For respected guests/invitees staying in the campus Wi-Fi access is given on demandbythecorrespondinghosts.Itispasswordbasedaccess.Passwordsare changed periodically by Technical Cell.
2. For others, some Wi-Fi can be accessible to all in specific areas like libraries etc with a per day limit on data on it.
3. Specific Wi-Fi installed in the department, if the Head of Department wants can give username password on request.

Wi-Fi Usage

1. The individual user will be responsible for his/her Wi-Fi usage.
2. Solicited and ethical usage is expected from the users.
3. The Internet Access through Wi-Fi is filtered access. Possible phishing, spurious, un solicited or obscene sites, gaming sites, some shopping/ multimedia streaming sites are blocked at firewall level.
4. There shall be a per day usage quota on Students User class.

5. TheuserswillaccesstheCollegeResourcesproperlyandwillnottrytoharm the resources.

Misuse and actions

a. If a user or his/her device is causing any harm to College resources or other users, then such a user will be warned by the concerned department or IT Cell. User's intention and device will be verified and the corresponding Head of the department will be informed accordingly.

b. A virus infected device may create noticeable network traffic or attempt cyber attacks.Thentheuserwillbenotifiedandhis/heraccessshallbeblockeduntil the infected device is cleaned/ free from viral infection.

Internet Access:

The User of a Net Access ID guarantees that the Net Access ID will not be shared with any one else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. Network IDs will only be established for students, staff and faculty who are currently affiliated with the College Students, staff and faculty who leave the College will have their Net Access ID and associated files deleted. No User will be allowed more than one Net Access.

In special cases like workshop/seminar/conferences etc. access could be permitted by prior permission of competent authority.

Limitations on the use of Resources/Data: On behalf of the College, IT Cell reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

Thedatadownloaded/livestreamlike(movie/video/songs/gaming/software etc)is not allowed.

Ethics and Etiquette: The User will not attempt to override or break the security of the College networks, or machines accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages.

CCTV Monitoring:

A. The system

✓ The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; Storage; Public information signs.

✓ Cameras will be located at strategic points on the campus, principally at the entrance andexitpointofsitesandbuildings.Nocamerawillbehiddenfromviewandallwillbe prevented from focusing on the frontages or rear areas of private accommodation.

✓ Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

✓ Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

B. Purpose of the system

✓ The system has been installed by the College with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to: Assist in the prevention and detection of crime.

C. The system will not be used:

- To provide recorded images for the world-wide-web.

D. The Security Control Room

✓ Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

✓No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers. Any other authorized member requiring access in special circumstances needs to get written permission from Principal..

✓ Staff, students and visitors may be granted access to the Control Room on a case- by-case basis and only then on written authorization from the Principal.

✓Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the center. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

E. Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

F. Recording

✓ Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

✓Images will normally be retained for **fifteen** days from the date of recording, and then automatically overwritten and the Log updated accordingly. Once a hard drive has

Reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

✓ All hard drives and recorders shall remain the property of the College until disposal and destruction.

4. Web Site Hosting Policy

For Official Pages: Sections and departments may have pages on college's official Web page. Official Web pages must conform to the College Web Site Creation Guidelines for Web site hosting.

For Personal Pages: Apart from Official profile on website, Faculty may request to have their personal pages linked to official website of the College by sending a written request to Technical Cell giving the details of the hyperlink of the URL that he/she wants to be added in the official website of the College . However, his/her pages must be used for the purpose of academics and should not violate any College, state, or central government laws. Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the College.

Supply of Information by Section, Department for Publishing on /updating the college Web Site:

Any Schools or Departments having any updated information should send a Hard Copy of such information duly signed by the competent authority/ Heads of Section, Department, or Division level, along with a softcopy to be sent to the IT Cell .

This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Section, Department, or Division. Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the webmaster upon receiving the written requests.

If such web pages have to be directly added into the official web site of the College, necessary content pages have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format.

Further, such requests along with the soft copy of the contents should be forwarded to the competent authority, IT Cell well in advance (3 days).

General Information Technology Usage Guideline:

a) Prohibited Use

Users must not send, view or down load fraudulent, harassing, obscene (i.e., pornographic),threatening, or other messages or material that are a violation of applicable law or College policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.

b) Copyrights and Licenses

Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the College’s information resources is a violation of this policy.

c) Social Media

Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.

d) Political Use

College information resources must not be used for partisan political activities prohibited by central, state or other applicable laws, and may be used for other political activities only when in compliance with central, state and other laws and incompliance with applicable College policies.

e) Personal Use

College information resources should not be used for activities unrelated to appropriate College functions, except in a purely incidental manner.

f) Commercial Use

College information resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages. Any such permitted commercial use should be properly related to College activities ,take into account proper cost allocations for government and otheroverheaddeterminations,andprovideforappropriatereimbursementtothe College for taxes and other costs the College may incur by reason of the commercial use.

g) Risks:

The College shall emphasize on managing the risks involved for the usage of IT resources. This shall include standard procedures for identification, minimization and monitoring of risk impact by preventive and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate internet connectivity for a fail-safe internet access.

h) Open Source Asset:

The College shall endeavor towards the promotion and effective usage of open source software.

i) Password Policy:

Passwords are a critical element in maintaining the security of IT assets. All client machines should have a power-on password and login password. Remember password features should not be used.

j) Safeguard your Equipment: Adopt Security measures that protect your equipment against theft, fire and explosives.

k) Protect your Power Supply: Protect your equipment from power failures and electrical anomalies.Makesurethatyourpowersupplieswillbeprovidedwithoutinterruptionand comply with the specifications provided by equipment manufacturers. Also consider multiple power feeds.

l) Secure your Cables: Protect your power lines and telecommunication cables from damage. Place power lines and telecommunication cables underground whenever those lines are connected to information processing facilities. Use Conduits to prevent unauthorized interception or damage to cables and lines.

m) Maintain your Equipment: Maintain your equipment to ensure that it functions properly. Follow the equipment manufacturers recommended maintenance specifications. Allow only authorized maintenance people to service your equipment and suggest keeping a record of all preventive and corrective maintenance activities.

5. Purchase/Procurement Policy

The policy is to establish the procedure for the purchase of computer hardware, software, networking equipment and allied material.

Procedure:

The purchase of computer hardware, software, networking equipment and allied material shall be done after the approval from the Central and Departmental Purchase committee. A member nominated by IT Cell (In charge) will be part of CPC/DPC for this purpose. The technical cell will check the minimum configuration and warranty of the above said and may suggest accordingly.

The purchase procedure shall be as per the College rule.

Warranty: Procurement of IT Assets should cater for onsite warranty, as far as practicable for extended period. The warranty should cover all items of non-consumable nature including batteries of UPS, laptops and such other portable IT devices. The scope of warranty of Software should also include patches, updates/upgrades and associated changesofapplicationandprovisionofhelpdeskfacilityforprovidingsupportinstructured and time bound manner.

Condemnation and Disposal of IT equipment:

The present disposal and condemnation policy follow the Guidelines vide circular No. 8-11/2012-13/IT-Idated26/12/2014 o f Department of Telecommunications, Ministry of Communications &IT, Government of India and Notification No. F.No.29-6/2018-S&S dated 25/11.2022 issued by Ministry of Education, Department of Education, and Government of India

Applicability

These guide lines will be applicable to all IT equipment installed in college.

Note:

i) Consumable items related to IT like used printer cartridges etc. are not included in the scope of scrapping on account of the fact of its nature as consumable.

ii) IT items like pen drives/floppies, which are petty valued and are not capitalized, are not qualified for the detailed scrapping procedure.

Grounds for Condemnation:

The IT equipment can be condemned on following grounds:

a) Equipment which has become obsolete technology-wise and can't be upgraded and support from vendors, either paid or unpaid, does not exist and their use may result in insecurity threat/ unauthorized access to data.

b) Beyond economical repair: When repair cost is considered too high (exceeding 50% of residual value equipment taking depreciation into account), and the age of the equipment. Such cases should be dealt on a case-to-case basis and should have concurrence of finance. Incase of IT equipment depreciationof20%peryearmaybe taken for calculation of residual value.

c) Equipmentthathasbeendamageddueto fireoranyotherunforeseenreasonand have been certified as beyond repair by the authorized service agency and agreed upon by the IT.

Disposal:

A. Such equipment shall be disposed strictly following the procedure as laid down in Rule196 to 201 of GFR 2005 [General Financial Rules of Government of India available here https://doe.gov.in/order-circular/general-financial-rules-2005] and notification regarding disposal of E-Waste issued by Ministry of Environment, Forests, and Climate Change [available here https://cpcb.nic.in/e-waste/]. Once the equipment has been condemned, it should be removed from office use and kept in the area allocated for scrapped equipment. College will also ensure removal of service and inventory labels from such equipment. AMC, if any, for such equipment /instruments shall be stopped with the effective date of scrapping. Essential data, if any ,must be removed after taking proper backup and preserved by the user of the equipment.

B. The IT cell shall propagate the information [in the form of notice, demonstration, relevant videos etc.] on disposal of E-waste to all users [regarding their personal E-waste] through various departments once in a year as a part of an awareness programme.

Procedure:

a) Scrapping proposals will be initiated by the user section/IT, which will be compiled by the IT Advisory Committee for further processing for scrapping.

b) End-user department/section/IT Advisory Committee will prepare "IT equipment condemnation note" in the pro-forma attached as Annexure-I.

c) Department/section/TechnicalCellwillconstituteacondemnationcommitteewhich will review the condemnation notes and recommend the condemnation of equipment asperapprovedguidelines.TheCommitteeshouldhaveatleastonememberfromthe TechnicalCell(forproposalsinitiatedbydepartment/section)andonefromthefinance wing.

d) All procedures and rules of the government on maintenance of records for condemnation of non-consumable items will be adhered to in these cases.

e) The condemnation report so prepared shall be put up for approval. The condemnation will be done only after recommendation of the IT committee and approval is obtained from competent authority.

Responsibilities of IT Cell:

A. Campus Network Back bone Operations:

a. The campus network backbone and its active components are administered, maintained and controlled by IT Cell

b. IT Cell operates the campus network backbone such that service levels are maintained as required by the College Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings’ Network

a. Physicalconnectivityofcampusbuildingsalreadyconnectedtothecampus Network back bone is the responsibility of IT Cell .

b. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of IT Cell. It essentially means exactly at which location the fiber optic-based backbone terminates in the buildings will be decided by the IT Cell. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity

c. shouldbeoffiberoptic,wirelessoranyothermedia)isalsotheresponsibilityof IT Cell IT Cell will consult with the client(s) to ensure that end-use requirementsarebeingmetwhileprotectingtheintegrityofthecampusnetwork backbone.

d. It is not the policy of the College to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the College's Internet links.

C. **Network Expansion:** Major network expansion is also the responsibility of IT Cell. Every 3 to 5 years, IT Cell reviews the existing networking facilities, and needs for possible expansion. Network expansion will be carried out by IT Cell when the College makes the necessary funds available. As IT is the essential component for every day life of College, funds shall be readily available.

D. **Wireless Local Area Networks:** Where access through Fiber Optic/UTP cables is not feasible, in such locations IT Cell considers providing network connection through wireless connectivity.

E. **Providing Net Access IDs and email Accounts:** IT Cell provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the College upon receiving the requests from the individuals.

F. **Network Operation:** IT Cell is responsible for the operation of a centralizedNetworkOperation.ThecampusnetworkandInternetfacilitiesareavailable 24/7aweek.Allnetworkfailuresandexcessutilizationarereportedtothe IT Cell technical staff for problem resolution.

G. **Network Policy and Technology Standards Implementation:** TECHNICAL CELL is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

H. **Receiving Complaints:** IT Cell may receive complaints from the users if any of the users is not able to access the network due to a network related problem at the user end. Such complaints may be generally through phone call/Mail/Complain Register to IT Cell. The designated person in IT Cell receives complaints from the users and coordinates with the user/service engineers or with the internal technical team to resolve the problem within a reasonable time limit. IT Cell will be responsible only for solving the network related problems or services related to the network. IT Cell may also receive suggestions for the smooth and timely delivery of services.

I. **Disconnect Authorization:** IT Cell will disconnect any section, department or division for routine maintenance for networking and its related issues. IT Cell will be constrained to *disconnect any Section, department, system or division from the campus network backbone* whose traffic violates practices set forth in this policy or any network related policy. If a Section, department, or division is disconnected, IT cell shall inform the concerned and shall provide the conditions that must be met to be reconnected.

J. **Enforcement:** TECHNICAL CELL periodically scans the College network for provisions set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines. Such disconnection shall be informed to the concerned individual and shallalsobeinformedonconditionsforreconnection.Incaseofdisconnectionormajor fault the IT cell shall inform the departments through mail or bulk messages regarding disconnection and reconnection.

K. The IT Cell (In charge) will be responsible for allocation of roles to the personnel under technical cell for better functioning of IT related issues in COLLEGE.

L. Where feasible, Technical Cell Head is to enforce these policies by System Configuration.

M. BackingupCriticaldataandapplicationresidingonServerswhileensuringsafecustody and accounting of media used for it.

N. AllthecomputersthatwerepurchasedbytheCollegecentrallyshallbehandedover totheTechnicalCell.TechnicalCellwillthenreceivetherequisitionanddistribute,and Technical Cell will also attend the complaints related to any maintenance related problems.

Responsibilities of Department or Sections

A. AnyCentre,department,orSectionorotherentitycanconnecttotheCollegenetwork using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the College The user account will be provided by IT Cell, upon filling up the prescribed application form and submitting it to IT Cell

B. Each Section, department, or division should identify at least one person as a Point of Contact and communicate it to IT Cell so that IT Cell can communicate with them directly in case of any network/system related problem at its end.

C. For any defective data storage device/IT assets like hard drive, pen drive etc are to be physically destroyed before dumping or throwing.

Policy Monitoring

Policy Dissemination

a. The IT Committee of the Prananath College(Autonomous), Khordha should ensure proper dissemination of this policy.

b. TheITCommitteemayusenewsletters,banners,bulletinboardsetc.tofacilitate increased awareness about this policy amongst their users.

c. Orientation programs for new recruits shall include a session on this policy.

d. For implementation of this policy, the IT cell shall be competent to suggest modifications in rules and the College will amend necessary rules as Suggested by IT cell or other wise from time to time.

Violation of Policy:

Any violation of the basic objectives and are as mentioned under the IT Policy of the College shall be considered as a violation and as a misconduct and gross misconduct under College Rules. Access Control Policy: Without permission mobile phones or any gadgets or electronic photography devices are not allowed in restricted or prohibited areas or in confidential documents rooms. Users are encouraged to be vigilant and to report any suspected violation of this policy immediately to the concerned office.

Review and Monitoring of Policy:

ThePolicydocumentneedstobereviewedatleastonceintwoyearsandupdatedifrequired, so as to meet the pace of the advancements in the IT related development in the industry.

Review of this policy document shall be done by a committee chaired by the Vice Chancellor or his Nominee of the College and all the members of the IT Committee. The College reserves all rights to relax the terms of this policy, further when required review of this policy document shall be done by committee.

Change Management

IT Policy necessarily evolves with changes in IT infrastructure and threat scenario. Once promulgated, further changes in IT policy would be reflected as additions/deletions to this document. Anything that is not covered in this policy will be decided by the Principal. The Principal has authority to interpret this policy and any decision taken by the Principal will be final and binding on everyone.

Committee

The IT and System Committee

The IT Committee shall be an apex advisory and recommending body on all matters pertaining toITintheCollegeandshallreporttocompetentauthority.ItshallbemandatoryforTechnical Cell to seek recommendation on all matters pertaining to College IT planning, maintenance, procurement and disposal prior to putting forward the proposal to competent authority. Investigators/co-investigators, planning to acquire and manage IT assets as well as department/section, who intend to develop and manage IT resources within the department may seek assistance from IT & System Committee.

The IT Committee shall consist of

- Principal Chairperson,
- Coordinator IQAC,
- IT Cell (In charge) as Member System Analyst– (Member),
- Senior Technical Teacher (Technical Cell) –Member .
- Two Professor from the College,

The committee may invite or co-opt additional members from outside as per need with the permission of Chairperson.

Function:

TheDepartment/CentreCommitteeshallhavethefollowingfunctions,namely–

(a) to advise and recommend on proposals for the development & procurement of new infrastructure, software, computers and other IT equipment for College end-user, students and for the general-purpose computer labs;

(b) To evaluate & advise on proposal for annual maintenance;

(c) To advise and recommend on proposals of ERP/intranet, ICT equipment & Smart boards, design and development of website and portals;

(d) ThecommitteeshallprovideadviceonITfacilities/software/hardware/internet/Wi-fi access for the College as well as matters pertaining to planning, purchase, utilization, maintenance and disposal.

Meetings:

MeetingsoftheITCommitteeshallbeconvenedatleasttwiceinayearbytheChairperson.

Attheendofthefinancialyear,TechnicalCellshallsubmittotheITCommitteeacopyofannual statementofexpenditureonITitems,andnewlyaddedanddisposedstocksforbetterplanning and assessment of status of IT infrastructure in the campus.

The proceedings of the IT Committee shall be submitted to the competent authority.

Others:

TheITpolicyofthecollegerespectstherighttoprivacyofeveryindividual concerned.

TheITcellwillhavethemandatetospreadawarenessregardingcyberfraud,password protection etc.

The vacancies in the IT cell shall be reviewed and filled on priority basis.

As NEP2020 has special focus on Indian languages, IT cell shall take necessary steps to help all concerned departments to implement it subject to the resources available.

Principal
Pranananth College (Autonomous),
Khordha

Principal
PRANANATH COLLEGE
(Autonomous)
KHORDHA