



# **KAZI NAZRUL UNIVERSITY, ASANSOL.**

## **IT Policies & Guidelines** **(Release: Jan. 2020 Version 1.0)**

**Prepared by  
ICT Cell,  
Kazi Nazrul University,  
Asansol, Paschim Bardhaman - 713340.**



## ***Kazi Nazrul University***

### ***IT Policy Ver. 1.0***

It has always been our endeavour to provide all faculty, students and staff with a modern, fully networked IT environment for academic and official use.

The **ICT Committee** has framed the following **KNU IT usage Policy**.

The users of KNU networking and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility as well as protect the privacy and security of the system. In case of complaints, appropriate action to be taken will be decided by the concerned Disciplinary committee in consultation with the competent authorities of KNU.

1. Faculty, staff, and students with authorized accounts may use the IT facilities for academic purposes, official business, and for personal purposes so long as such use
  - does not violate any law, University policy or IT act of the Government of India.
  - does not interfere with the performance of University duties or work of an academic nature.
  - does not result in commercial gain or private profit other than that allowed by the University.
2. Users are expected to respect the privacy of other users and they must **not allow any other person to use their password or share their account**. It is the users' responsibility to protect their account from unauthorized use by changing passwords periodically and using passwords that are not easily guessed. Sharing of passwords for any purpose whatsoever is strictly prohibited.
3. Users should exercise care while **entering their passwords** at other non-trusted sites and should not be misled by **purported emails from admin or other IDs without verifying the email IDs**.

4. Any attempt to bypass system security, guess others' passwords, or in any way gain unauthorized access to local or network resources is forbidden. Users may not use another person's account, attempt to forge an account identity, or use a false account or e-mail address.
5. Transferring copyrighted materials to or from the KNU systems without express consent of the owner is a violation of international law. In addition, use of the internet for commercial gain or profit is not allowed. If done so, it will be sole responsibility of the user. **Downloading of copyrighted movies/books/games** via any means is punishable and users are forewarned that on receipt of any complaints appropriate disciplinary action will be taken.
6. Downloading and installing of new software has to be done with the explicit consent of the respective facility in-charges. Installation of unlicensed software on KNU facilities, or on individual machines connected to the KNU network, is strictly prohibited.
7. Setting up of any facility requiring password transmission over clear text is prohibited without TLS/SSL encryption.
8. Users are encouraged and expected to use only their official email addresses provided by KNU for all official communications. Any complaints/requests to ICT must be made using your authorized email id otherwise we will not entertain your request. In case, for some reason, a user is not able to access his/her official email then s/he may write to us from his/her registered alternate mail id with us.
9. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. Chain letters are not allowed. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly disallowed. Subscribing to mailing lists outside the University is an individual's responsibility. Subscribing someone else to any group outside KNU is illegal.
10. It is forbidden to send frivolous or academically unimportant messages to any group. Broadcast of messages to everyone in the system is allowed only for academic purposes and emergencies. Violations of this (as decided

by competent authorities) will result in immediate freezing of user's account for an extended period as determined by the authorities.

11. Shared email accounts for any purpose whatsoever are not allowed. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the university authorities, must have a single responsible user.
12. Recreational downloads and peer to peer connections for recreational purposes are banned.
13. To the extent possible, users are expected to connect only to the official KNU WiFi network for wireless access. Setting up of unsecured WiFi systems on the KNU network is prohibited in accordance with a Government of India ban.
14. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.
15. NO FOOD OR DRINK is permitted in the KNU laboratories. Smoking is strictly prohibited. Also making noise either through games/ music or even talking and/ or singing loudly is prohibited.
16. Playing of Games in University computing laboratories is strictly prohibited.
17. Display of offensive material (either on computer screens or through posters etc.) is strictly disallowed and serious action will be taken against offenders.
18. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the concerned disciplinary committee may take an action by issuing a warning through disabling the account and for routine infractions; appropriate fines/penalties will be levied. In case of repeat offenders or other extreme cases the user may be prohibited access to IT facilities at KNU, and/ or other appropriate action as determined by University authorities.
19. The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately or as deemed fit by the competent authorities of the university after a brief announcement by any means, e-mail, printed notices, etc.

### ***Privacy Policy for IT usage at KNU***

Keeping in mind the internal security requirement of KNU, applicable Law and to ensure as far as possible full privacy for all legitimate use of KNU IT facilities to all students, staff, faculty and visitors, the following **Privacy Policy has been framed:**

#### ***Use of encrypted channels and digital certificates***

1. All facilities in KNU that require users to provide their passwords are set up over encrypted channels (https/SSL/TLS) using strong encryption.
2. All encryption facilities are signed using a valid Certificate which the users are advised to verify before providing their passwords.

#### **Privacy of User data & Meta-data**

1. As a general rule KNU will respect users privacy regarding their data and meta-data. No KNU administrator will directly access user data such as mail or other stored content. Automated tools may process some of this for backup and other routine functions as well as relevant statistics and usage collection. In addition, automated malware/anti-spam tools may access the data to flag any illegal/malicious content and or mine the metadata to build relevant usage details.
2. The administrators follow a policy of never accessing the content of any mailbox or user data or access details, unless required (or instructed) to do so as a part of an investigation of any misdemeanour. Certain automated scripts/programs may report IT usage violations which may require investigation. Also in case of a formal complaint either internal, or received externally from law enforcement agencies, the access logs/email records/ other user data may be examined by authorized KNU personnel only to investigate the complaint. Such investigations would typically require the consent of the competent authorities of the university.

#### ***Email privacy***

1. All users including faculty, staff and students are provided an official email id in the domain knu.ac.in. According to KNU policy all users are expected to use this email id in all official correspondence.
2. Mail exchange with all clients is carried out over a secure G-suite encrypted channel.
3. Mail exchanges with other servers outside KNU are carried out using opportunistic TLS encryption. The exchange is encrypted if the other server supports it, and is over a plain text channel otherwise. Decryption keys for all encrypted transfers will be provided to designated law enforcement agencies only if such requests are in accordance with the IT Act of the Government of India.
4. Automated programs may be run by administrators to generate performance statistics and/or to train tools for spam and misuse detection. The administrators follow the policy of never examining the contents of the log to determine who sent mails to whom unless they are required to do so as a part of investigation of misdemeanour.
5. All transactions (not merely authentication) should be carried out using the secure https protocol (over SSL).
6. The authenticity of any email that is accepted cannot be guaranteed by the mail transfer protocol. All users are advised to cross check, in case of doubt, or use digitally signed emails. In case emails are digitally signed, the authenticity is certified by the certificate provider and it is the user's responsibility to verify the certificates.

### ***Web server privacy***

1. The web accesses, if KNU has its own web server, would be logged for 26 weeks after which they would be automatically deleted. The logs may be mined to generate access and performance statistics. The logs would be accessible to the administrators who normally never examine them manually unless required to do so for the purposes of investigation of misdemeanour or debugging.
2. The third party who is responsible for the development/maintenance/hosting of KNU's website need to ensure the same and a non disclosure agreement with all pertinent clauses should be signed and reviewed at periodic intervals.

## ***Proxy-server privacy***

1. All users may access the web through the KNU proxy server (on availability of KNU proxy server), where they are required to provide their passwords. The passwords are never logged.
2. Access of pornographic and other offensive web-sites should be blocked by the proxy-server (on availability of KNU proxy server). The access control list is downloaded periodically from standard sites which maintain upgraded lists of sites providing offensive contents. However, these mechanisms are not entirely fool-proof.
3. The accessed pages should be cached unless there are explicit 'direct' directives from the web servers. The cached pages are neither mined nor examined. However, such examinations may be carried out for investigation of misdemeanour.
4. Web access records of all users should be logged for 26 weeks after which they are automatically deleted. Mining of the logs may be carried out automatically to generate performance and usage statistics. Also, the data may be mined automatically to determine the top down-loaders of the day. If such downloads are perceived to be unreasonable (by the administrators) then an explanation may be sought from the user. The policy of manual examination of the logs by the administrators is similar to that of the mail logs described above.
5. Please note that in the case of a complaint (see Privacy of user data & Metadata bullet 2 above) the access logs may be examined by authorized KNU personnel to investigate the complaint. In case the concerned Disciplinary Committee and university authorities deem necessary as per applicable law, the impugned access details may be provided to the concerned external agencies.

## ***Privacy of passwords***

1. The passwords are maintained on the servers in encrypted format.
2. The administrators may run standard password crack software on the encrypted passwords if required under dire situations.
3. The KNU will normally never request the users for their passwords, and the users are expected to protect their passwords against any form of phishing. In case the KNU requires the users to register their passwords for some facility, such request will be made through duly authenticated or hard copy notices signed by appropriate authority.

## **Security**

No Quality of Service guarantees for security can be given. However, the following routine precautions are adopted.

1. Only administrators would be authorized to login to the mail, web, proxy and other servers (on availability of these servers).
2. Security advisories on the software currently being used (OS components, antivirus, etc) should be regularly monitored. At least one designated system administrator should receive an email alert whenever such an advice is released by the official maintainers of the software. The software should be updated periodically and whenever required.
3. All ports except those necessary for functioning of the servers (on availability of these servers) should be blocked (firewalled) both from outside and inside.
4. Standard intrusion detection software is run on the LAN to monitor any change of MAC addresses corresponding to IP addresses of trusted machines. A designated administrator automatically receives an email alert in such cases.
5. The administrators would carry out routine checks to spot unusual access patterns on a 'best effort' basis.

## ***Network access and monitoring policy***

KNU is required by the IT Act 2009 and the GOI guidelines to be able to associate every internet access using its facilities to specific users and maintain logs of all such accesses for a minimum period of three months.

## **Wifi routers and access points**

1. Installation of unprotected WiFi routers is banned by a GOI regulation.
2. Installation of Wifi routers in the academic area will not be permitted without explicit consent from KNU. All users should use the authorized KNU\_WIFI SSIDs for Wifi access.
3. All WiFi routers that provide connection to the KNU LAN should have at least WPA2-PSK (pre-shared key with WPA2 encryption) standard security enabled.



4. The GOI regulation prohibits shared access of WiFi resources and mandates WiFi access only through a central authentication mechanism. In view of this, 802.1x (WPA2-Enterprise) is the minimum acceptable standard for setting up Wifi access in the **academic area**.

### **Connecting other ISP networks to KNU LAN**

It is strictly prohibited to connect other ISP networks (not obtained through KNU) to the KNU LAN without explicit consent from KNU.

### **VPN and ssh access to KNU LAN**

It is strictly prohibited to setup unauthorized VPN or ssh access facilities for connecting to KNU LAN from outside without explicit consent from KNU. The VPN facility available at KNU should be used for such purposes. It is also prohibited to facilitate external access to the KNU network using any terminal sharing or other similar software.

### **Access monitoring in KNU VLANs**

ARP monitoring is to be enabled on all VLANs and all IP address to MAC address mappings will be logged and maintained for a period of three months.

### **Network usage monitoring in KNU**

Usage of KNU's network (wired & wireless) will be monitored on daily/weekly schedule and excess usage may incur financial penalties or suspension of privileges.

### **Internet access from academic area (wireless LAN)**

Connecting to the SSIDs *KNU WIFI*, will require 802.1x authentication and all wireless network traffic will be encrypted using WPA/WPA2 standards. All authentications will be logged along with time of access, uid of the user, registered DHCP IP address and the MAC address of the accessing device.

Since connections to KNU WiFi are authenticated, access to services on all other safe ports (except port 25) will be open and made available through NAT/PAT at the KNU firewall. VPN connectivity for popular protocols will also be enabled at the firewall where logs will be maintained. The logs will include the time of access and the NAT/PAT mappings.

All logs will be maintained for a period of minimum three months.

### **Internet access from the Wifi SSID *KNU\_GUEST/KNU\_Guests***

The Wifi SSID *KNU\_GUEST/KNU\_Guests* will be made available throughout the academic area on special recommendation.

It will be responsibility of the account creator to verify the identity of the guest and record the mobile phone number of the guest, as per GOI guidelines, at the time of creating guest accounts. KNU will set up a facility to communicate the password to the guest through SMS on the recorded mobile phone.

### **Static IP addresses for inward connections**

On special requests static external IP addresses may be allocated to specific servers for access from outside on specific ports. This may be required for designated web servers and other research facilities. In all such cases it will be the responsibility of the facility in-charge to install proper firewall and security measures to ensure that the access is restricted to the specific server and the KNU network is completely protected from external accesses. No shell or VPN access should be provided without explicit consent of KNU.

### **Unrestricted external access from designated servers**

Unrestricted access to internet bypassing the proxy servers may be given from specific servers on request for special research and operational needs. It will be the responsibility of the facility in-charges to ensure that

1. access to such a facility is restricted and users do not use such a facility to access the internet bypassing the proxy servers
2. KNU IT usage policy and privacy policy are strictly adhered to.
3. Access logs are maintained for accesses on all ports as required by GOI regulations.

### **Password reset policy**

Please note that safekeeping of the password is primarily the responsibility of the user. Please be careful while entering your KNU password. Users should be discouraged to refrain from making frivolous requests for password reset.

### **Proxy for Internet Access**

Intranet/Internet Web Browsing:

1. Intranet web browsing is free, and is not accounted for.
2. You will be asked for your credentials, please authenticate yourself with your username and password.

3. If your login is successful, you can surf the Internet as long as this window/tab is open - you can browse from another tab or window.

## Phishing Warning

- Phishing is the fraudulent practice of sending emails pretending to be from reputable sources to steal passwords or sensitive personal or financial information or to install malware on the target's computer.
- Even if you receive emails that appear to have come from KNU official or System Admin asking for userid or password, for any reason, you are not supposed to give any information.

## Certificates

All KNU facilities that require users to provide their passwords should be set up over secure TLS/SSL encrypted channels. Setting up of encrypted TLS/SSL connections require the server to present SSL certificates to the client, so that the client may authenticate the server. This is to prevent against possible man in the middle attacks. **Please note that accepting a server certificate without verifying its authenticity makes a user vulnerable to attacks.**

## Internet access for visitors

For contract employees, all faculty members and designated staff from the departments/centers would be provided user accounts on joining/application as per instruction from competent concerned authority.

## KNU campus Wifi

1. The KNU has released Wifi solution for the entire academic and administrative areas. These services would be accessible with SSIDs.
2. We would use IEEE 802.1x (WPA2 Enterprise) based encryption for security on KNU WIFI.

## Windows software

KNU provides Windows software to its users through the [Microsoft Open Value Subscription Agreement for Education Solutions](#). Licensed Windows software under this

agreement can be installed in University machines for use by all faculty, students and staff of KNU.

- [Windows/Office installation and activation](#)
- [Windows software distribution](#)
- [List of software under Microsoft campus agreement](#)
- [Windows update service](#)
- [Terms of use](#)

## **Windows/Office installation and activation**

### **Prerequisites**

Windows Volume License is for upgrades only. Before you try to upgrade, you must first purchase an underlying, qualifying, and genuine Windows license. For more information, visit the following Microsoft website: <http://www.microsoft.com/piracy/knowthefacts/legalizationsolutions.aspx>

**While procuring hardware from OEM it is important to ensure that you have purchased an underlying, qualifying, and genuine Windows license which can be upgraded under the volume license agreement.** This may require you purchase a low cost starter kit from the OEM. Please get in touch with the OEM in case of any doubt.

### **MATLAB**

**It is an interactive platform for numerical computation and data visualization, which along with its programming capabilities provides a very useful tool for almost all areas of Science and Engineering.**

**Current Version: R2018b**

**We have campus license agreement with MATLAB.**

**Users can install network based licenses (10,000 licenses for *all* toolboxes), or standalone individual licenses.**

**For Operating Systems : Windows, Linux, and Mac(64-Bit ) (see system requirement)**

## **VPN for Faculty/Staff/Students**

We would have future plans to provide support for VPN (virtual private network) for connecting to the KNU internal LAN from outside KNU.

## **Video Surveillance Policy**

- *The system comprises of Fixed position cameras; Pan Tilt and Zoom cameras*
- *Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be 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.*
- 1.4 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.

### **Purpose of the system**

The system has been installed by university 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:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

### **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 unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry..
- Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorisation from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.
- Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

## **Website Policy**

### **Preamble**

A University Website means any website created, maintained, or managed by the University (or a website created, maintained, or managed by a third party appointed/hired by the University) through which the University conducts various official operations/functions. University Websites do not include (i) faculty members' personal websites, (ii) student organization websites, and (iii) students' personal websites.

University Websites have evolved into an excellent medium of information propagation and promote visibility of that University. The university web sites serve as the primary information source for both the aspiring candidates who want to join and the existing students to better harness the resources hosted in the University web page and should support the vision, mission, goals, and traditional academic values of the university.

With the phenomenal increase in adaptability of digital medium for information delivery, we need to set certain key policies to govern/ensure that the University website follows certain norms/guidelines to not only ensure data privacy, data protection but also an internal process for authentic information to be uploaded on the website as well as minimize scope for redundant data.

The website: [www.knu.ac.in](http://www.knu.ac.in) is the official website of Kazi Nazrul University. designed, developed and hosted by a third party under the aegis of Kazi Nazrul University.

Technicalities:

**S/W used** (Frontend as well as Backend) - PHP, MySQL, Laravel Web Framework

**Security:**

- a) OWASP Application security risks will be taken care in the coding.
- b) Sophos Central Intercept X Server End point security implementation
- c) Web application Firewall implementation
- d) Quarterly Vulnerability assessment and Penetration testing activities and mitigation of open items

**Space Allocated for the new website** - 30 GB Space and it is scalable

**Data Backup** - Once in every 3 days

**Privacy policy:**

Any site that gathers any data about its users, even if it is simply through tracking their location, is required to have a privacy policy.

A privacy policy is a statement contained on a website that details how the operators of the site will collect, store, protect, and utilize personal data provided by its users. The definition of personal data includes names, addresses (physical or e-mail), IP addresses, telephone numbers, date of birth, and financial information, such as debit or credit card details, etc. In addition to outlining how the University will use the information, it also includes a disclaimer how it will meet its legal obligations, and how those sharing their data can seek recourse should the company fail to meet those responsibilities.

Resolution - A text section of our website telling students, faculty and visitors what data we collect from them and also explains how we use it.

*Disclaimer: Though all efforts have been made to ensure the accuracy of the content on this website, the same should not be construed as a statement of law or used for any legal purposes.*

*The KNU website does not automatically capture any specific personal information from you, (like name, phone number or e-mail address), that allows us to identify you individually. If you are being requested to provide personal information, you will be*

*informed for the particular purposes for which the information is gathered and adequate security measures will be taken to protect your personal information.*

*We do not sell or share any personally identifiable information collected from the user(s). Any information provided to the website will be protected from loss, misuse, unauthorized access or disclosure, alteration, or destruction.*

*We may gather certain information about the User, such as Internet protocol (IP) addresses, domain name, browser type, operating system, the date and time of the visit and the pages visited. We shall make no attempt to link these addresses with the identity of individuals visiting our site unless an attempt to damage the site has been detected.*

*These principles require that the data collected be limited to only that which is entirely necessary for the purpose of the site; how individuals may access their data; how the information is protected; and the accountability of the data collector.*

### **Copyright Policy:**

All electronic publication of University follows legal standards regarding copyright and trademarks. University shall obtain permission when including copyrighted or trademarked material such as text, photographs, audio, video, graphics, or company names or logos, and include a permission statement or disclaimer as required by the owner.

*Disclaimer: Though all efforts have been made to ensure that there is no copyright infringement with respect to the content on this website, the same should not be construed as a statement of law or used for any legal purposes.*

*Links to other websites that have been included on this Website are provided for public convenience only. KNU is not responsible for the contents or reliability of linked websites and does not necessarily endorse the view expressed within them. We cannot guarantee the availability of such linked pages at all times.*

*These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the exclusive jurisdiction of the courts of India.*

Material featured on this website may be reproduced free of charge after taking proper permission by sending a mail to us. However, the material has to be reproduced accurately and not to be used in a derogatory manner or in a misleading context. Wherever the material is being published or issued to others, the source must be prominently acknowledged. However, the permission to reproduce this material shall not extend to any material which is identified as being copyright of a third party.



Authorisation to reproduce such material must be obtained from the departments / copyright holders concerned.

### **Hyper Linking Policy**

Links to external websites:

At many places in this website, you may find links to other websites/websites. This links have been placed for your convenience. KNU is not responsible for the contents and reliability of the linked websites and does not necessarily endorse the views expressed in them. Mere presence of the link or its listing on this website should not be assumed as endorsement of any kind. We can not guarantee that these links will work all the time and we have no control over availability of linked pages.

Links to KNU website by other websites

We do not object to you linking directly to the information that is hosted on this website and no prior permission is required for the same. However, we would like you to inform us about any links provided to this Website so that you can be informed of any changes or updations therein. Also, we do not permit our pages to be loaded into frames on your site. The pages belonging to this Website must load into a newly opened browser window of the User.

Links to other websites that have been included on this Website are provided for public convenience only. KNU is not responsible for the contents or reliability of linked websites and does not necessarily endorse the view expressed within them. We cannot guarantee the availability of such linked pages at all times.

These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the exclusive jurisdiction of the courts of India.

### **“Uploading/Deleting of information/documents on website” related Policy:**

- Any uploading on the website has to be the responsibility of the System administrator.

The procedural flow of interdepartmental information/direction with respect to the new website would be as follows:

#### **Office of the Registrar**

| <b>Activity</b> | <b>Point of Origin</b> | <b>Approving Authority</b> | <b>Concurrence</b> |
|-----------------|------------------------|----------------------------|--------------------|
|-----------------|------------------------|----------------------------|--------------------|

|  |               |  |  |
|--|---------------|--|--|
| Admission  | Registrar     |  |  |
| Registration   | Registrar     |  |  |
| I Card Distribution of Students & employees  | Dy. Registrar |  |  |
| Recruitment  | Registrar     |  |  |
| Statutory/Non Statutory committees   | Dy. Registrar |  |  |
| HRM (Leave, PF, Payroll, Posting, Appointment, Promotion, Retirement, Service Book, pay scale) | Dy. Registrar |  |  |
| Commemorative Days, Events, celebrations, Convocation ceremony                                 | Dy. Registrar |  |  |
| Purchase & Tender  | Registrar     |  |  |
| University Holidays  | Dy. Registrar |  |  |
| MoU  | Registrar     |  |  |
| Alumni   | Registrar     |  |  |
| Fee structure  | Registrar     |  |  |
| Act/Statute/Ordinance/Regulations  | Registrar     |  |  |
| Publication  | Registrar     |  |  |

**Office of the Controller of Examinations**

| Activity           | Point of Origin | Approving Authority | Concurrence |
|--------------------|-----------------|---------------------|-------------|
| Pre-Examination    | Dy. Controller  |                     |             |
| During Examination | Dy. Controller  |                     |             |
| Post Examination   | Controller      |                     |             |
| Convocation Data   | Controller      |                     |             |

**Office of the Finance Officer**

| Activity     | Point of Origin | Approving Authority | Concurrence |
|--------------|-----------------|---------------------|-------------|
| Semester fee | FO              |                     |             |

|                         |    |  |  |
|-------------------------|----|--|--|
| notification – Campus   |    |  |  |
| Rates/Quotation         | FO |  |  |
| Hostel Fee Notification | FO |  |  |
| <b>Tender</b>           | FO |  |  |

**Secretary, College Council**

| <b>Activity</b>                                | <b>Point of Origin</b> | <b>Approving Authority</b> | <b>Concurrence</b> |
|--|------------------------|----------------------------|--------------------|
| Admission Notification for application         | Secretary              | Registrar                  |                    |
| Pub. of merit list                             | Secretary              | Registrar                  |                    |
| Admission notification according to merit list | Secretary              | Registrar                  |                    |
| Verification Notification                      | Secretary              | Registrar                  |                    |
| Class Commencement Notification                | Secretary              |                            |                    |
| Pub. of Academic Calendar                      | Secretary              |                            |                    |
| Notification to Colleges other than IC         | Secretary              |                            |                    |
| Notification to Department                     | Secretary              |                            |                    |
| Curriculum                                     | Secretary              |                            |                    |
| Syllabus                                       | Secretary              |                            |                    |
| End of Admission Notification                  | Secretary              | Registrar                  |                    |
| Termination of class notification              | Secretary              |                            |                    |

**Librarian**

| <b>Activity</b>                             | <b>Point of Origin</b> | <b>Approving Authority</b> | <b>Concurrence</b> |
|---|------------------------|----------------------------|--------------------|
| Central Library related notifications       | Librarian              |                            |                    |
| Central Library related various content     | Librarian              |                            |                    |
| Addition of electronics and print resources | Librarian              |                            |                    |

|   |           |  |  |
|---|-----------|--|--|
| to Central Library                                    |           |  |  |
| Library fine/fee related notification                 | Librarian |  |  |
| Addition of new service notification                  | Librarian |  |  |
| Central Library related events like orientation, etc. | Librarian |  |  |

### ICT

| Activity         | Point of Origin | Approving Authority | Concurrence |
|------------------|-----------------|---------------------|-------------|
| Any Notification | ICT Head        |                     |             |

### Estate Officer (EO)

| Activity                                      | Point of Origin | Approving Authority | Concurrence |
|---|-----------------|---------------------|-------------|
| Repair and Maintenance Notification (if any)  | EO              |                     |             |
| Power Management notification                 | EO              |                     |             |
| ALL AMC notification                          | EO              |                     |             |
| Cleanliness                                   | EO              |                     |             |
| Furniture related                             | EO              |                     |             |
| Training Programmes/ Seminars/ Workshops, etc | EO              |                     |             |
| Security                                      | EO              |                     |             |
| University vehicles related                   | EO              |                     |             |
| <i>***Other notifications as per statute</i>  |                 |                     |             |

**Development & Planning Officer (DPO)**

| <b>Activity</b>                  | <b>Point of Origin</b> | <b>Approving Authority</b> | <b>Concurrence</b> |
|----------------------------------|------------------------|----------------------------|--------------------|
| Scholarship related notification | DPO                    |                            |                    |
| Grants/Funding related           | DPO                    |                            |                    |

**Training & Placement Officer**

| <b>Activity</b> | <b>Point of Origin</b> | <b>Approving Authority</b> | <b>Concurrence</b> |
|-----------------|------------------------|----------------------------|--------------------|
| Training        | TPO                    |                            |                    |
| Placement       | TPO                    |                            |                    |

**System administrator**

| <b>Activity</b> | <b>Point of Origin</b> | <b>Approving Authority</b> | <b>Concurrence</b> |
|-----------------|------------------------|----------------------------|--------------------|
| Server Downtime | System Administrator   |                            |                    |

**Response/Turnaround Time on Uploading/Deleting of information/documents on the website**

- For uploading of regular notices/circulars on the website, the maximum turnaround time would be **4 hrs**, if the email direction is provided within 5:30 pm of a working day. Otherwise, the email direction would be regarded as received on the next working day and the maximum turnaround time would be 4 hrs from 10 AM of the next working day.
- In the case of an exigency and the notice/circular needs to be uploaded immediately then it needs to be documented clearly and the direction would be given due importance and the notice/circular would be uploaded as soon as possible.
- For updation of a departmental webpage, the maximum turnaround time would be 2 days, if the email direction is provided within 5:30 pm of a working day.

Otherwise, the email direction would be regarded as received on the next working day and the maximum turnaround time would be 2 days from 10 AM of the next working day.

- For updation of a departmental webpage or any other webpage, the maximum turnaround time would be 2 days, if the email direction is provided within 5:30 pm of a working day. Otherwise, the email direction would be regarded as received on the next working day and the maximum turnaround time would be 2 days from 10 AM of the next working day.

### **INSTITUTIONAL EMAIL ID POLICY**

1. Every employee of Kazi Nazrul University who are appointed in substantive posts will be provided an institutional email id, with the domain: knu.ac.in, for the purpose of official communication with the University.
2. The norm to be followed for the different stakeholders are as follows:
  - a. **For employees:**
    - Substantive Category: Institutional Email Ids would be provided as a privilege for joining the institution.

N.B.: No casual/part time/ guest faculty will be issued institutional email id

**b. For students:**

A student/research scholar will be provided with an institutional email ID, only if s/he needs an institutional email ID for academic purpose such as availing of scholarship/fellowship or publication of research papers, etc. during his/her study/research at the University.

3. The Institutional Email Ids would be created as per the following standards from the date of approval of the policy:
  - a. **For Teachers** :Short form of Name of the department (as used in curriculum for coding).(dot)First name of the teacher@domain name (knu.ac.in).  
**Eg.:** Santanu Banerjee, Assistant Professor, Dept. of English, mail id will be – [eng.santanu@knu.ac.in](mailto:eng.santanu@knu.ac.in)

- b. **For Officers:** short form of designation.(dot)@domain name (knu.ac.in)  
**Eg.:** Rahul Majumdar, Secretary College Council, mail id will be – [scc@knu.ac.in](mailto:scc@knu.ac.in)
  - c. **Non-Teaching Staff: (Substantive):** First Letter of First Name.(dot)Last Name@domain name (knu.ac.in).  
**Eg.:** Arindam Bouri, Cash Assistant, mail id will be – [a.bouri@knu.ac.in](mailto:a.bouri@knu.ac.in)
  - d. **Head of the Department:** hod.(dot)name of the department@domain name(knu.ac.in).  
**Eg.:** Head of the department. Applied Psychology, mail id will be – [hod.appliedpsychology@knu.ac.in](mailto:hod.appliedpsychology@knu.ac.in)
  - e. **Deans:** dean.(dot)name of the faculty@domain name (knu.ac.in)  
**Eg.:** Dean, Faculty Council of Postgraduate Studies in Commerce, mail id will be – [dean.commerce@knu.ac.in](mailto:dean.commerce@knu.ac.in)
4. The creation of Groups for group mail would be as per the following standard:
- a. **Deans Group:** All deans will be the members of this group.
  - b. **All Officers Group:** All Officers will be the members of this group.
  - c. **All HoDs Group:** All the Heads of the Academic Departments will be the members of this group.
  - d. **All Employees Group:** All employees of the University (Teachers + Officers + Non-Teaching staffs (*Substantive only*)) will be the members of this group.
  - e. **All Employees Group (*Substantive only*):** All substantive employees will be the members of this group.
  - f. **All Non-Teaching Staff Group:** All Non-Teaching Staffs (*Substantive only*) will be the members of this group.