



गौतम बुद्ध विश्वविद्यालय ग्रेटर नोएडा, गौतम बुद्ध विश्वविद्यालय

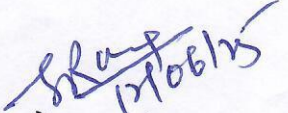
जी.बी.यू./009/सी.सी.सी/07/2025- 363

दिनांक:- 12/06/2025

::सूचना::

सक्षम स्तर द्वारा प्रदत्त अनुमोदन दिनांक 28/02/2025 के अनुपालन में गठित समिति द्वारा गौतम बुद्ध विश्वविद्यालय के लिए GBU IT Policy के क्रियान्वयन एवं आई.टी. सेवाओं को और अधिक सुदृढ़ एवं प्रभावी बनाने के उद्देश्य से संस्तुतियाँ की गयी हैं। उक्त संस्तुतियों पर सक्षम स्तर से प्राप्त अनुमोदन के क्रम में गौतम बुद्ध विश्वविद्यालय हेतु GBU IT Policy इस सूचना के साथ समस्त संकाय सदस्यों, शिक्षणेत्तर अधिकारियों/कर्मचारियों एवं विद्यार्थियों के अनुपालनार्थ संलग्न है।

संलग्नक: यथोपरि।


(डा० शोभा राम)
उप-कुलसचिव

प्रतिलिपी:

1. मा० कुलपति महोदय के स्टाफ को महोदय के संज्ञान में लाने हेतु।
2. कुलसचिव महोदय को सूचनार्थ।
3. समस्त अधिष्ठाता/प्रभारी अधिष्ठाताओं/विभागाध्यक्षगणों को सूचनार्थ।
4. प्रभारी छात्र कल्याण को सूचनार्थ।
5. मुख्य छात्रावास अभिरक्षक (पुरुष) को सूचनार्थ।
6. मुख्य छात्रावास अभिरक्षक (महिला) को सूचनार्थ।
7. सिस्टम मैनेजर को इस आशय से प्रेषित कि उक्त सूचना को विश्वविद्यालय के समस्त संकाय सदस्यों, शिक्षणेत्तर अधिकारियों/कर्मचारियों एवं छात्र व छात्राओं को ई-मेल के माध्यम से प्रेषित किये जाने एवं विश्वविद्यालय वेबसाइट पर प्रमुखता से प्रकाशित किये जाने हेतु।
8. सम्बन्धित पत्रावली/गार्ड फाइल।


उप-कुलसचिव



IT POLICIES

**IT Policies
And Procedures
Of
Central Computer Center
GAUTAM BUDDHA UNIVERSITY**

Introduction

At Gautam Buddha University (GBU), the Central Computer Center (CCC) recognizes IT resources as a crucial component of the university infrastructure, requiring meticulous management to ensure their security and availability for teaching staff, non-teaching staff, research scholars, and students. To fulfill this objective, the university has established fundamental IT security policies and standards aimed at providing authorized users with both access and reasonable security. The GBU IT Policies and Procedures are designed to facilitate and support authorized access to university information.

The purpose of the GBU IT Policies and procedures is:

- To establish Protocols for Information Security at University level.
- To identify and prevent the opposing rules of Information Security and misuse of IT resources.
- To satisfy University legal and ethical responsibilities about its IT resources.
- To establish Distribution Policy for distributing IT equipment's to the teaching/non-teaching staff.
- To enable the University to respond to complaints and queries about any violation of law with the University IT Policies and Procedures.
- These policy applies to all users of computing resources owned or managed by the university. Individuals covered by the policy include university officers, faculty and guest faculty, staff, students, alumni, guests, external individuals, and any other entity who fall under the management of the university accessing network services via computing facilities of the university. Users will not violate any law, university IT policy, or IT act of the Government of India.

Responsibility

Authorized Users of GBU IT resources are personally responsible for adhering to all University policies, procedures, and standards concerning Information Security, irrespective of their campus, schools, or location. They will be held personally accountable for any misuse of these resources. It is the responsibility of every GBU user to familiarize themselves with the University IT Policies and Procedures and ensure compliance with them. When an individual utilizes University IT resources and accepts any computing/IT accounts issued by the university, they thereby agree to adhere to this policy and all other computing-related policies. It is the individual's

responsibility to stay informed about any changes in the university's IT policy and to adjust to these changes as required from time to time.

About Central Computer Center

The Central Computer Center is a central facility that caters to the computing needs of faculty, staff, and students. This facility operates 24x7 throughout the year, serving as the hub for computer-related services on the campus. It is well-equipped with advanced computers, necessary peripherals, and essential software. Additionally, the Central Computer Centre is equipped with power backup through two high-end 80KVA UPS units and backup is provided by centralized generator set. Air conditioning is provided by a precision AC & VRV AC plants & power backup is provided by the Centralized generator set.

- Linux/Windows desktops are accessible in all classrooms across various school labs to facilitate e-learning and interactive lab sessions during classes. The CCC network backbone operates on Fiber Optic connectivity, interconnecting the CCC, Schools of Studies, and administrative offices. The access network utilizes structured UTP network infrastructure incorporating approximately 400 units of 10/100 Mbps switches. The University is equipped with a 2 Gbps bandwidth for Internet connectivity obtained from the National Knowledge Network (NKN) and other ISPs.
- CCC offers easily accessible and excellent computational facilities to both faculty and students, boasting over 870 computers that cater to their academic, research, and recreational needs. The center maintains outstanding internet connectivity. The entire campus is interlinked through LAN and seamless wireless connectivity, facilitated by access points, which are managed by the WLC (Wireless LAN Controller). Indoor APs are strategically installed to ensure connectivity across various buildings, including different schools within the University.
- NextGen Firewalls are installed to detect Malware, Spyware, and viruses at the gateway level, thereby securing the network from potential threats.
- Multiple servers are installed in the CCC data center for various applications used by different schools and labs.

GBU IT Network Policy

- 1) The GBU IT Network, which includes Internet, Intranet, and along with associated computer/networking equipment, software, and accounts, is the property of the University. It is designated solely for GBU academic purposes and to serve the interests of the University and all Authorized Users.
- 2) Authorized Users are responsible for maintaining the security of their passwords and accounts. Passwords must be kept confidential and not shared with any other individual.
- 3) All devices connected to the GBU IT Network must have password-protected screensavers with automatic activation set at 10 minutes or less, or users must log off when the device is not in use.
- 4) Authorized Users must take special care to protect laptops and desktops connected to the GBU IT Network in accordance with security guidelines provided by the University.
- 5) All authentications will be logged, including the time of access, user ID, registered DHCP IP address, and MAC address of the accessing device.
- 6) Logs will be maintained for a maximum period of three months.
- 7) Unauthorized installation or distribution of copyrighted software or materials is strictly prohibited on official devices or devices connected to GBU network.
- 8) Unauthorized copying of copyrighted material, including digitization and distribution of photographs, music, or software, is strictly prohibited.
- 9) Exporting software, technical information, or technology in violation of export control laws is illegal and requires approval with university administration.
- 10) Introduction of prohibited software into the GBU IT Network, including unauthorized VPNs, P2P applications, and viruses, is strictly prohibited.
- 11) Transmitting material over the GBU network that violates sexual harassment or hostile workplace laws or university policies is strictly prohibited at any social platform
- 12) Making fraudulent offers of products or services from a University account or computer connected to the GBU IT Network is prohibited.
- 13) Causing security breaches or disruptions of communication over the GBU IT Network, including unauthorized access to data, is strictly prohibited.
- 14) Port scanning or security scanning is prohibited without prior agreement/permission to Information Security.
- 15) Unauthorized network monitoring of GBU network that intercepts data not intended for the Authorized User is prohibited unless part of the user's normal job duties.
- 16) Interfering with user authentication or security of any device, network, or account is strictly prohibited.
- 17) Interfering with or denying service to any user other than the individual's host is prohibited.
- 18) Sending messages or executing commands with the intent to interfere with or disable a user's terminal session is prohibited.

- 19) Wi-Fi/Internet facility will be provided only on laptops for students and outsourced staff, with a limit of one device per person. Faculty and staff are allowed a maximum of three devices.
- 20) Installation of personal Wi-Fi routers in academic/housing/other areas is strictly prohibited without prior permission from CCC.
- 21) Installation of personal Wi-Fi routers in hostel areas is strictly prohibited. If such installations are discovered, CCC reserves the right to collect the router and the user's network port related services will be blocked for 6 months or a fine of Rs. 2000/- may be imposed or enforce both penalties, or taken any other action decided by the competent authority.
- 22) Connecting non-CCC networks to the GBU LAN without explicit consent from CCC is strictly prohibited.
- 23) CCC is authorized to take reasonable steps to ensure compliance with network-related policies and protect the integrity and security of the campus network backbone. The Central Computer Centre reserves the right to close the Internet connection of any user violating the IT policy or impacting computing resources for other users.
- 24) Violations of GBU IT policies, including illegal downloads of copyrighted content, will result in appropriate fines, legal action, or suspension of Internet privileges.
- 25) Electronic communication systems using the GBU IT Network are for official University purpose only and must comply with University IT policies and procedures.
- 26) Users are prohibited from engaging in any activity through websites or applications aimed at circumventing network filtering or carrying out any other unlawful acts that could compromise the network's performance or security.
- 27) The CCC may block content over the Internet that contravenes the relevant provisions of the IT Act 2000 and other applicable laws, or poses a security threat to the network.
- 28) The CCC may implement filtering systems to block or limit access to specific social media sites or content deemed inappropriate or unrelated to academic and professional activities or believes may negatively impact users' productivity.
- 29) Individual departments/individuals connecting to the university network over the LAN may run server software, such as HTTP/Web server, any school application server, FTP server, only after obtaining written permission from the CCC and ensuring compliance with the university IT policy for running such services. Failure to comply with this policy constitutes a direct violation of the university IT policy and will result in termination of their connection to the network.
- 30) Access to remote networks (Any desk, Team viewer, SSH, Telnet etc.) using a University's network requires prior permission from CCC to connect the system. Connection must comply with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.
- 31) The CCC will be compelled to disconnect client machines if potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

- 32) All user IDs on the GBU network are non-transferable and cannot be shared or used by other than intended user. Any such use is a violation of GBU policy, and the concerned user will be held responsible.
- 33) The CCC has the sole prerogative to terminate network connections to computers within its domain temporarily; and permanently after due approval for frequently such activities for actual abuse of the network and/or its components..

GBU Website policy

- 1) Website policy outlines the guidelines for creating, managing, and maintaining the university's websites to ensure consistency, accessibility, security, and accuracy of information. It applies to all university departments, faculty, staff, and third-party involved in web content creation and management.
- 2) This policy applies to all websites, webpages, and online services hosted on the university's domains or branded as part of the university. It includes official university websites, departmental pages, research project sites, and other web-based applications or services.
- 3) All university websites are the property of the university. Each department or unit is responsible for the content on their respective webpages, ensuring it aligns with university standards and policies.
- 4) Website committee in collaboration with the school website communications team, will oversee the overall structure, design, and functionality of the university's web presence. Content owners within departments are responsible for keeping their webpages up to date and compliant with university guidelines.
- 5) Updating of the new content or significant changes to existing content should be approved by competent authority/Dean of the school/department head.
- 6) CCC will conduct regular accessibility audits to identify and rectify issues, ensuring continuous compliance with accessibility standards.
- 7) GBU websites must implement appropriate security measures to protect personal data and sensitive information. This includes the use of SSL certificates, encryption, and secure login protocols.
- 8) Any third-party services or tools integrated into university websites must be reviewed and approved by the website committee to ensure they meet security and accessibility standards.

GBU Domain Email IT policy

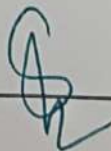
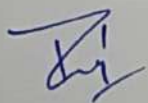
- 1) The Email Facility should primarily be used for academic and official purposes, with limited use for personal matters.
- 2) To create a university domain email account, users are required to fill out the designated form.
- 3) Any postings made by Authorized Users from a University Email address must include a disclaimer stating that the opinions expressed are strictly those of the author and not necessarily those of the University, unless the posting is related to University academic purposes.
- 4) Authorized users are prohibited from sharing their email accounts with others. Individual account holders are personally accountable for any misuse of their email accounts.
- 5) Authorized users should configure messaging software (such as Outlook Express or any client app) on their primary computer to periodically download

emails from the mailbox onto their computer. Users are responsible for backing up incoming and outgoing emails from their account.

- 6) Impersonating email accounts of other users is considered a serious offense under the university IT security policy.
- 7) Sending unsolicited email messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material (Email SPAM) is strictly prohibited.
- 8) Email account can be locked if the account has been found to be sending out malicious emails.
- 9) Any form of harassment via Email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages, is strictly prohibited.
- 10) Unauthorized use or forging of Email header information is strictly prohibited.
- 11) In the case that a password is lost or forgotten, the user can approach with the written application or email to the CCC to request the generation of a temporary password. The user must present sufficient credentials for this purpose.
- 12) Mass emailing's over the GBU IT Network from the University email account must be approved by the relevant authority before sending. The approval must be noted at the bottom of the email and include the name of the approving individual and the date of approval.
- 13) The University's email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments.
- 14) The CCC won't ask users for their passwords. Users should keep their passwords safe from phishing and cyber-attack.
- 15) Upon completing the necessary clearance process and receiving 'No Dues' confirmation from the CCC, or upon leaving the university or any deputation, the email account will remain active for an additional 15 days. During this time, users can back up any important emails or data they wish to keep. After this period, the email account will be deleted or suspended from the server.
- 16) Student email account remains valid for the duration of your course validity. It is to be used solely for academic purposes and should not be utilized for any other activities or personal use.
- 17) Any official group email will be sent to everyone through circular@gbu.ac.in after approval by the competent authority, and school-level group emails will be sent after approval by the Dean.

Access to Social Media Sites from GBU Network

- 1) The utilization of social networking sites by GBU users is regulated by the "Framework and Guidelines for use of Social Media for Government Organizations." Or guidelines issued by GBU time to time.
- 2) Users are obligated to comply with all relevant provisions outlined in the India IT Act 2000 when disseminating information on social networking sites.
- 3) Users must adhere to the "Terms of Use" stipulated by the respective social media platform/website, as well as observe copyright, privacy, defamation, contempt of court, discrimination, harassment, and other applicable laws.
- 4) Users must consistently employ high-security settings on social networking sites.



- 1) The CCC will only be responsible for resolving hardware-related issues or problems with operating systems or any other application software that has been legally purchased by the university through CCC.
- 2) If the CCC or its technical person encounter any applications that are disrupting network operations or contravening the IT policies of the university, such incidents should be reported to the CCC and university authorities.
- 3) The IT helpdesk provides support via phone, remote tool and in-person, with self-service resources also available for common issues.
- 4) IT services will be available during standard operational hours, typically Monday to Friday or as university working days, 9:30 AM to 5:30 PM.
- 5) Emergency IT support is available 24/7 for critical issues affecting core operations.

No Dues Policy

- 1) All users must obtain a "No Dues" clearance from the University Computer Center before leaving the university
- 2) All issued desktops and laptops, along with peripherals and accessories, must be returned in good working condition.
- 3) CCC staff will inspect all returned equipment for functionality and check for any damage or missing components.
- 4) Users are financially responsible for any repair or replacement costs for damaged or lost equipment.
- 5) Users must back up their data before returning devices, as all data will be erased upon return, CCC is not responsible for any data backup.
- 6) Users must contact the CCC to schedule the return and clearance process.
- 7) Ensure all equipment is cleaned, all personal data is backed up and removed, and all components (chargers, cables, etc.) are included. A "No Dues" certificate will be issued only after the return, inspection, and approval of the equipment condition.

Monitoring and Privacy

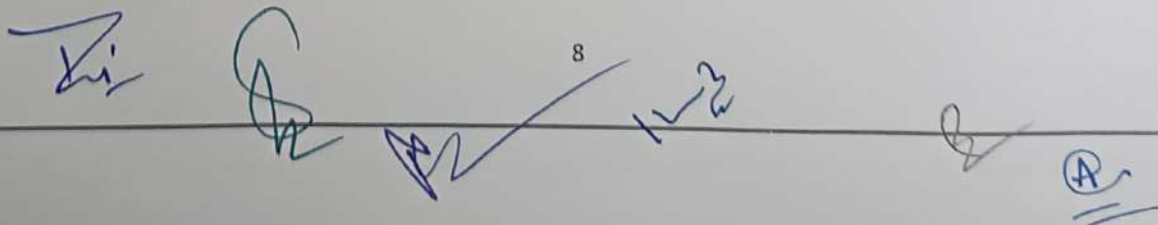
- 1) The CCC shall possess the authority to conduct audits arbitrarily or with due permission on networks and systems at regular intervals, commencing from the point of adherence to this policy.
- 2) The CCC, for reasons pertaining to security or compliance with relevant laws, reserves the right to access, review, copy, or delete any form of electronic communication or files stored on University-provided devices, with notification provided to the user. This includes but is not limited to files, emails, posts on any electronic media, and Internet history.
- 3) The CCC may engage in the monitoring of users' online activities on the University network, subject to the Standard Operating Procedures outlined by Government of India norms.
- 4) Monitoring of network traffic to detect unauthorized access and malicious activities.
- 5) Collection and analysis of system logs for troubleshooting, security auditing, and performance monitoring.

- 5) The User shall not post any material that is offensive, threatening, and obscene, infringes upon copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or otherwise unlawful.
- 6) The User shall not disclose or utilize any confidential information acquired in their capacity as an employee of the university.
- 7) The User shall not make any comments or post any material that could potentially harm GBU's reputation.
- 8) The university may implement filtering systems to block or limit access to specific social media sites or content deemed inappropriate or unrelated to academic and professional activities.

Desktop/Software/Any other Peripherals Policy

- 1) Any computer purchases made by individual departments/projects must ensure that such computer systems have all licensed software (including operating system, antivirus software, and necessary application software) installed.
- 2) In accordance with the anti-piracy laws of India, the University's IT policy prohibits the installation of any pirated or unauthorized software on university-owned computers and on computers connected to the university campus network. In the event of any such instances, the university will hold the department or individual personally responsible for any piracy.
- 3) An individual user is personally accountable for the proper utilization of all resources allocated to them, encompassing the computer, network address or port, software, and hardware. Consequently, they are responsible to the university for all activities involving these resources.
- 4) User will not attempt to access restricted areas of the network, desktop, operating systems, security software, or other administrative applications without obtaining proper authorization from the system owner or administrator.
- 5) IT devices provided by the university to a user are intended primarily for academic, research, and other university-related purposes, and must be used in a lawful and ethical manner. This includes the use of desktop devices, portable devices, external storage media, and peripheral devices such as projectors, Wi-Fi, copiers, printers, and scanners, among others.
- 6) Users must ensure that updated virus-scanning software is running on all systems. Exercise caution when opening email attachments from unknown senders, as they may contain viruses, fishing email, or Trojan.
- 7) Users must not exchange any devices with each other without prior permission from the CCC to maintain accurate stock records; otherwise, users will be held responsible for any misuse or damage resulting from unauthorized exchanges.
- 8) If a user requires any equipment, such as desktops, printers, laptops, cartridges, network devices, or their parts, they must submit a proper request to the CCC duly signed by Dean of the school or Head of the department of admin section. Upon receipt of any parts through a CCC challan, the user must immediately submit a signed copy of the CCC challan. Failure to do so will result in the CCC not providing any further equipment or parts to the user.

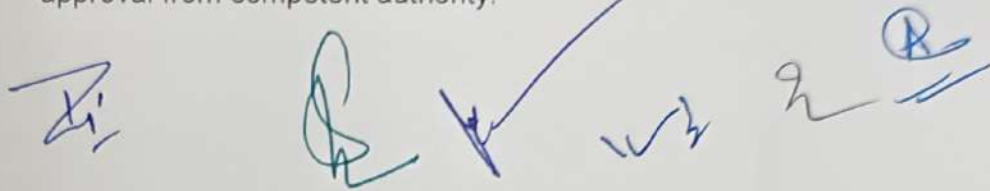
Scope of Service

The bottom of the page contains several handwritten signatures and initials in blue ink. From left to right, there is a signature that appears to be 'Di', a large stylized signature, a signature with the number '8' written above it, a signature that looks like 'V2', a signature that looks like 'b', and a circled 'A' with a double underline.

- 6) All network monitoring data will be handled in accordance with data protection regulations and secured against unauthorized access.

Review and Amendments

- 1) This policy will be reviewed annually and amended as necessary to ensure it remains relevant and effective in supporting the university's IT needs.
- 2) The IT Policy Review Committee, comprising representatives from the IT department, legal team, and other competent authority, shall oversee the review process.
- 3) Emergency amendments will be implemented immediately, with retrospective approval from competent authority.

Five handwritten signatures in blue ink are arranged horizontally. From left to right: a stylized signature, a signature with a large loop, a signature with a checkmark-like flourish, a signature with a wavy line, and a signature with a circled 'A' and a checkmark.

Asset Ownership and Management

- All IT equipment's/assets issued to employees shall remain the property of the university. The employee is considered the custodian of the equipment during their tenure or assignment and is responsible for its proper usage.
- All issued IT Equipment's (desktops, laptops, peripherals, and accessories) must be returned in working condition, except for normal wear and tear and repairable faults/disfunctions.
- If any hardware component of the IT Equipment fails after issuance, the faulty part may be replaced by the CCC, subject to the availability of that part either in the market or from CCC stock.
- If the IT equipment is beyond repair, it may be replaced with another available unit from CCC stock.
- In case the Equipment cannot be repaired, the concerned individual must return the issued IT equipment to the CCC. The CCC will initiate the process of scrapping the equipment in accordance with the university's e-waste policy and UP Government regulations.
- All IT equipment/software purchased by the university must be recorded in the CCC inventory prior to issuance to any individual, department, or school. This ensures uniform standards, proper maintenance, and efficient asset management.
- In cases where IT equipment is lost or damaged due to negligence, the concerned employee may be held financially liable, as per the university's rules and policies.
- A No-Dues Clearance from the CCC shall be mandatory for employees seeking final clearance upon exit from the university.
- The relocation of any IT equipment's/peripherals by a user, department, or school must be accompanied by a formal written information submitted to the CCC. No IT equipment shall be issued without prior notification to the CCC.
- The end-of-life process for IT equipment shall be in accordance with the policies established by the Government of Uttar Pradesh.

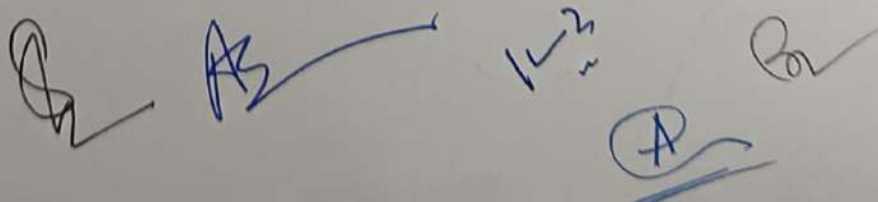
All students admitted to Gautam Buddha University shall be issued official university email IDs upon completion of the admission process.

Standard Email Format:

- Regular students: rollno@gbu.ac.in
- Ph.D. students: name.phddeptname@gbu.ac.in

The Admission Office shall provide student details in the specified format.

Sr. No.	Student Name	Roll No.	Course & Branch	Admission Year	Email Alias (suggested)



The final list of students shall be provided by the concerned department/school after the first semester examination.

If any student is left out, they may apply for an email ID through their department/school. The application must be forwarded to the CCC by the respective Head/Dean.

Deactivation of Student Email IDs and IT Facilities may occur under the following conditions:

- When the student applies for no-dues clearance.
- Upon receiving a verified list from the school.
- If inactive for one year, the email ID may be deleted by the CCC.



1/23





All Forms

Li, Q, P, W, H, R



CCC FORM NO: -

DATE:-

Gautam Buddha University
Central Computer Center
Email Registration Form for Students

- 1) Name:
- 2) Enrollment No.....
- 3) School Name:
- 4) Correspondence Email ID:
- 5) Communication Address:
.....
- 6) Mobile No:
- 7) Attachment: GBU ID Card

The above information is true to the best of my knowledge. I will also undertake to abide by all rule and regulations of the Central Computer Center.

(Signature of Student)

Note: - GBU email account remains valid for the duration of course validity. It is to be used solely for academic purposes and should not be utilized for any other activities or personal use. Any usage beyond the specified scope will result in appropriate action being taken in accordance with the GBU IT rule.

Recommended By (HoD)

I hereby approve the above name person to have a student email account.

(Signature of HoD with Stamp)

(Signature of System Manager)

CCC Use Only

FORM NO:

Email ID: -

Password: -

(The above password is temporary and will be automatically changed upon the user's first login prompt.)

Created By:

(Signature of Technical Superintendent)

[Handwritten signatures and initials in blue ink]



CCC FORM NO: -

DATE:-

Gautam Buddha University Central Computer Center

Email Registration Form for Faculty/Staff/Others

- 1) Name:
- 2) Employee ID:
- 3) Designation:
- 4) School/Department Name:.....
- 5) Correspondence Email ID:
- 6) Communication Address:
- 7) Mobile No: Office Ext. No:
- 8) Nature of Job (Permanent/OCFD/Contract):

The above information is true to the best of my knowledge. I will also undertake to abide by all rule and regulations of the Central Computer Center.

Attachment: GBU Appointment letter

(Signature of User)

Recommended By (Dean/Hod)

I hereby approve the above name person to have an official email account.

(Signature of Dean/Hod with Stamp)

(Signature of System Manager)

CCC Use Only

FORM NO:

Email ID: -

Password: -

(The above password is temporary and will be automatically changed upon the user's first login prompt)

Created By:

(Signature of Technical Superintendent)



**Gautam Buddha University
Central Computer Center**

CCC Application No.....

Date:

To

The System Manager
Central Computer Center
Gautam Buddha University

Subject: - Complaint request for Repair of Desktop/Laptop/ Printer/Projector/Network.

Sir,

This is to inform you that the Desktop/Laptop/Printer/Projector/Network is not working properly. Issued to individual/ School/Lab/ Department. Details are as follows:

- Device Model No. Device S.No.
- Initial Problem Description

Signature of User

Name:.....

Designation:.....

Department:.....

Room No:.....

Mobiie No:.....

System Manager
(Signature & Seal)

Assigned to:-

Name:.....

Technical Superintendent
(Signature & Seal)

- Device Status.....
- Technician Remark

(Technician Signature)

[Handwritten signatures and marks]



CCC FORM NO: -

DATE:-

Gautam Buddha University

Central Computer Center

Wi-Fi Device Registration Form for Students

1) Name:

2) Roll No.:

3) School/Hostel Name:

4) Correspondence Email ID:

5) Mobile No:

6) Permanent MAC Address:

(Note: 1:-Steps to get the MAC address: Windows: 1. Go to Start->Run 2. Type CMD and press Enter key 3. In the prompt type: "ipconfig /all" 4. Note down the "Physical Address for Wireless LAN Adapter" as the MAC address. Linux: 1. Launch the Terminal by hitting "CTRL+ALT+T" keys simultaneously 2. Type "ifconfig | grep HWaddr" and press Enter key
2:- Steps to get the MAC Address: Android: 1. Go to setting > About > Status > MAC Address, Apple: 1. Setting > General > About > Wi-Fi Address)

7) Device Type (Laptop/Other):

8) Device Brand and Model No.....

DECLARATION

The above-mentioned device belongs solely to me, and I shall be responsible for all use of this device on the network. I commit to using this facility for academic purposes only and will not share my account with others. I understand that any misuse of the IT infrastructure of Gautam Buddha University constitutes a violation of University regulations and may result in administrative or disciplinary actions (GBU IT Policy)

(Signature of User)

(Signature of Hod with Stamp)

(Signature of System Manager)

CCC Use Only

FORM NO:

SSID Name:-.....

Registration Date:-.....

(Signature of Technical Superintendent)

Li

Li

Li

Li



CCC FORM NO: -

DATE:-

Gautam Buddha University Central Computer Center

Wi-Fi Device Registration Form for Faculty/Staff/Others

- 1) Name:
 - 2) Employee ID:
 - 3) Designation:
 - 4) School/Department Name:
 - 5) Correspondence Email ID:
 - 6) Mobile No: Office Ext. No:
 - 7) Nature of Job (Permanent/OCFD/Contract):
 - 8) Permanent MAC Address:
- (Note: 1:-Steps to get the M A C address: Windows: 1. Go to Start->Run 2. Type CMD and press Enter key 3. In the prompt type: " ipconfig /all" 4. Note down the "Physical Address for Wireless LAN Adapter" as the MAC address. Linux: 1. Launch the Terminal by hitting "CTRL+ALT+T" keys simultaneously 2. Type "ifconfig | grep HWaddr" and press Enter key
2:- Steps to get the MAC Address: Android: 1. Go to setting > About > Status > MAC Address, Apple: 1. Setting > General > About > Wi-Fi Address)
- 9) Device Type (Laptop/Mobile/Other):
 - 10) Device Brand and Model No.

DECLARATION

The above-mentioned device belongs solely to me, and I shall be responsible for all use of this device on the network. I commit to using this facility for academic purposes only and will not share my account with others. I understand that any misuse of the IT infrastructure of Gautam Buddha University constitutes a violation of University regulations and may result in administrative or disciplinary actions (GBU IT Policy)

(Signature of User)

(Signature of Dean/Hod with Stamp)

(Signature of System Manager)

CCC Use Only

FORM NO:

SSID Name:-

Registration Date:-

(Signature of Technical Superintendent)





Gautam Buddha University
Central Computer Center
CALL REPORT

CCC Docket no. :	Date:	Call Logged Time:
Contact Persons Name:	Call Closed Time:	
Mobile No:	Ext No:	
Location/Address:		
Device Model No:	Device Serial No:	
Device Details:	Device Status:	
Complaint Description:		
Action Taken/Remark:		
User Remark:		
User Signature:	Name & Signature of Technician:	
CCC Authorized Signature:		

Li

[Signature]

[Signature]

[Signature]

123

[Signature]



Gautam Buddha University

Central Computer Center

CCC202411-CL

Delivery Challan

Date:

Handed Over To:

School/ Department,
Gautam Buddha University
Greater Noida

Contact person: _____
Designation _____
Phone:- _____

Handed Over By:-

Central Computer Center:
Gautam Buddha University
Greater Noida
0120-234-4246

Description: -.

S.No.	Part Model	Part Serial No.	Status	Qty.

Created By: Office Assistant

(Technical Superintendent)

(System Manager)

Handed Over To;
Name- :

(Signature with Seal)

Handwritten signatures and marks:

- Signature 1 (left)
- Signature 2 (middle-left)
- Signature 3 (middle-right)
- Signature 4 (top-right)
- Signature 5 (bottom-right)



Gautam Buddha University

Central Computer Center

No Dues Certificate

Date

Handed Over by:-

School/Department,
Gautam Buddha University
Greater Noida

Contact Person:-
Designation
Phone:-

Handed Over To:-

Central Computer Center;
Gautam Buddha University
Greater Noida
0120-234-6237

Description: -

S/No.	Device Name	Device Detail	Status	Qty.

Checked By: Technician

(Technical Superintendent)

(System Manager)

Handed Over By:
Name-

(Signature with Seal)

[Handwritten signatures and marks]



Gautam Buddha University
Central Computer Center

CCC Application No.....

Date:

To

The System Manager
Central Computer Center
Gautam Buddha University

Subject: - Application for Printer cartridge Refill.

Sir,

This is to inform you that my printer cartridge needs to be refilled. Details are as follows:

- Printer Model No.
- Printer S.No.
- Cartridge Sr.No.....

Signature of User

Name:

Designation:

Department:

Dean/HOD
(Signature & Seal)

System Manager
(Signature & Seal)

Cartridge Received By:-

Name:

Condition : Good- ☐ Damage- ☐

Sign:

For CCC Use Only

1. Issued Cartridge S.No.....
2. Issued Cartridge Model no.....
3. Register Request no.....
4. Issued Date
5. Refill/Recycle/New.....

(CCC Representative)