CRITERION 4- INFRASTRUCTURE AND LEARNING RESOURCES

4.4.2 Institution frequently updates its computer availability for students and IT facilities including Wi-Fi





BAREILLY INTERNATIONAL UNIVERSITY
(Established Under Govt. of U.P. Act 26 of 2016)
Rohilkhand Medical College Campus, Pilibhit Bypass Road, Bareilly-243006 (U.P.) INDIA
Phone: 0581-2526011-12, Fax: 0581 - 2303345
Email: info@biu.edu.in Website : www.biu.edu.in

4.4.2

Institution frequently updates its computer availability for students and IT facilities including Wi- Fi

Bareilly International University: Leading the Way with Advanced E-Content and IT Infrastructure

Bareilly International University (BIU) is a renowned institution offering undergraduate (UG) and postgraduate (PG) programs in **Medicine, Dentistry, Pharmaceutical Sciences, and Nursing**. BIU is committed to leveraging cutting-edge technology to enhance learning experiences, providing students and faculty with modern facilities for e-content development and top-notch IT infrastructure.

E-Content Development Facilities

1. **Media Centre-** The university's Media Centre is equipped with advanced tools for creating digital educational content. Faculty members utilize this facility to produce high-quality video lectures, presentations, and interactive learning modules. This enables students to access educational material anytime, making it easier to understand complex medical and healthcare concepts through dynamic, multimedia-driven resources.

2. **Audio-Visual (AV) Centre-** BIU's state-of-the-art AV Centre enhances traditional classroom learning by incorporating technology into the educational process. The AV Centre facilitates the creation of visually engaging content, such as practical demonstrations, clinical simulations, and interactive tutorials. This is particularly beneficial for medical, dental, nursing, and pharmaceutical students, where visual representation of procedures is crucial to understanding.

3. **Lecture Capturing System (LCS)-** BIU's Lecture Capturing System (LCS) allows the university to record live lectures and make them available online for students to revisit at their convenience. This system ensures that students can easily access lectures on-demand, whether for review or in case of missed classes, supporting flexible learning and deeper understanding of course material.

IT Infrastructure and Wi-Fi Access

1. **Wi-Fi Connectivity-** BIU offers comprehensive campus-wide Wi-Fi access, ensuring that students, faculty, and staff are always connected. With high-speed internet available across all academic and residential areas, students can access online learning resources, e-content, and research materials anytime and from anywhere on campus. This connectivity supports seamless access to the Learning Management System (LMS) and other digital platforms.

2. **State-of-the-Art IT Facilities-** BIU continuously upgrades its IT infrastructure to stay at the forefront of educational technology. The university provides well-equipped computer labs with the latest hardware and software, giving students access to essential tools for research, digital learning, and project work. These labs are particularly valuable for students in healthcare programs, where simulations, data analysis, and digital research are integral parts of the curriculum.

3. **Digital Media and Learning Management System (LMS)-** BIU integrates all its e-content—whether developed through the Media Centre, AV Centre, or LCS—into its robust Learning Management System (LMS). The LMS allows students to access lecture notes, video recordings, assignments, and discussion forums in a centralized platform. It also helps faculty track student progress and facilitate effective online interaction. The LMS, combined with reliable Wi-Fi and advanced IT facilities, ensures a seamless and enriched digital learning experience for students.

Conclusion

Bareilly International University's investment in e-content development, advanced IT infrastructure, and campus-wide Wi-Fi ensures a modern and flexible learning environment. By incorporating digital tools into its medical, dental, nursing, and pharmaceutical programs, BIU empowers students to excel in their fields and meet the demands of the rapidly evolving healthcare industry.

4.4.2

COMPUTING FACILITIES

YEAR	METRIC DETAILS
2020-2021	21000
2021-2022	163850
2022-2023	121435
2023-2024	76350
2024-2025	172890

LIST OF COMPUTERS

DEPARMENTS	NUMBER
ORAL PATHOLOGY	2
PEDIATRIC AND PREVENTIVE DENTISTRY	2
CONSERVATIVE AND ENDODONTICS	2
OMR	4
PROSTHODONTICS	2
ORTHODONTICS	4
PHD	1
ORAL SURGERY	1
PERIODONTICS	1
PRINCIPLE OFFICE	2
OFFICE	2
ADMINISTRATIVE OFFICE	1
GOVT SCHEME OFFICE	2
TOBACCO CENTRE	1
DENTAL STORE	1
PHARMACY	1
LAPTOPS	3
EXAMINATION CELL	2
TOTAL	34

INSTITUTE OF DENTAL SCIENCES

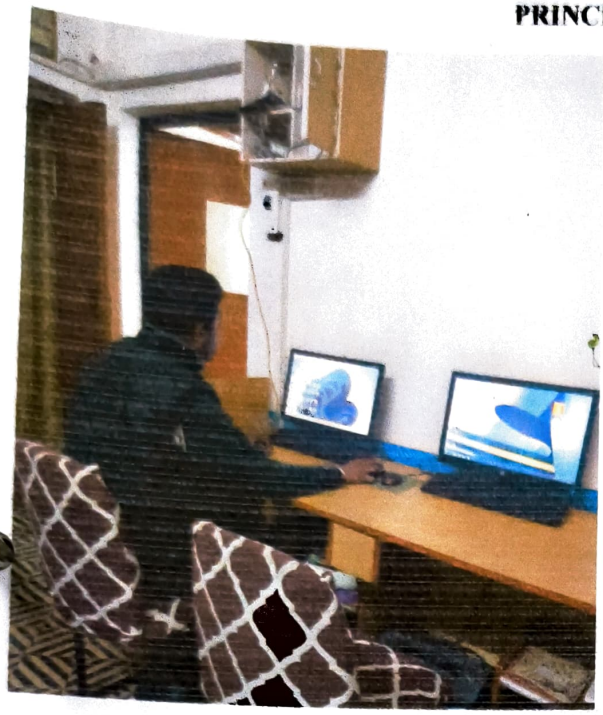
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY

Pillibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA

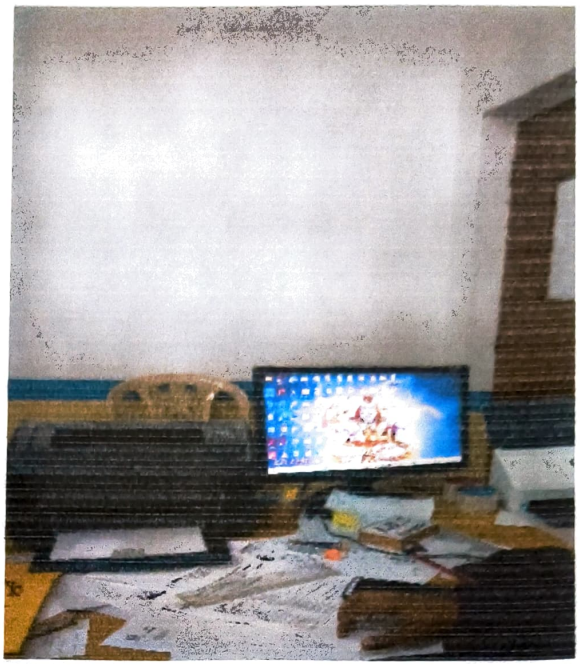
Website: www.idsbareillv.in E-mail ID: info@idsbareillv.in Contact No. 0581-2526244

S.NO.	DEPARTMENT	DESCRIPTION
1.	OMDR	2 MONITORS-17" HP,2CPU-DELL VOSTRO 3660, UPS-ELEMT 625 VA UPS, OPG PRINTER-DRYVIEW 5700, 1 CANON G570 PRINTER
2.	PROSTHODOCTICS	2 MONITORS- 15" DELL, 2 CPU -INSPIRON 30305,2 UPS- LAPCARE, 1 PRINTER HP INKJET 24334
3.	OMFS	1 MONITOR- ACER 15", 1 CPU- ACER VERITON, UPS- IBALL, 2 PRINTERS- HP INKJET 1018, HP INKTANK 319
4.	ENDO & CONS	1 MONITOR- 15" GATEWAY, 1 MONITOR- 15" HP, 1-CPU – COMPAQ PRESARIO 2023, 1 CPU – HP PAVILLION 23543, ,2 UPS- LAPCARE, 1 PRINTER- HP K209A
5.	PHD	1 MONITOR -DELL 15", 1 CPU- DELL INSPIRON 30305, 1 UPS ELEMT 475 VA, PRINTER-HP 1018
6.	ORTHODONTICS	1 MONITOR-DELL 15",1 MONITOR- HP 15", 1-MONITOR-ACER 15", 1 MONITOR- HP 17",1 CPU- HP COMPAQ PRO 6305, HP-280 PRO G6, 1 CPU- ACER VERITON, 1 CPU – HP PAVILION P2, 1 X-RAY PRINTER FUJIFILM DRY PIX LITE, 1 PRINTER – CANON LBP2900B, 1 PRINTER- EPSON L805, 4 UPS- IBALL, APC, MICROTEK, UNILINK
7.	PERIODONTICS	1 MONITOR -DELL 15", 1 CPU- DELL INSPIRON 30305, 1 UPS ELEMT 475 VA, PRINTER- HP K209A
8.	PEDODONTICS	1 MONITOR – HP 12", 1 MONITOR- HP 15", 1 CPU – COMPAQ PRESARIO 2024, 1 CPU- HP PAVILION 23, 2UPS – WEP, 1 PRINTER- HP 1018
9.	ORAL PATHOLOGY	1 TV MONITOR – LG, 1 CPU – COMPAQ PRESARIO 2022, 1- SMART BOARD COMPUTER- PROMARK, 1 MONITOR-LG 15", CPU- ACER VERTON, 1 UPS- IBALL, 1 UPS -APC, 1 PRINTER= HP 1018, 1 PRINTER- CANON G570
10.	EXAM CELL	2 MONITORS- 15" ACER, 2 CPU-VERITON, 2UPS- IBALL, UNILINK, 3 PRINTERS- HP INKTANK 319, CANNON- LBP-2900B, HP INKJET 1020
11.	OFFICE	2 MONITORS- 15" ACER, 2 CPU-VERITON, DELL INSPIRON 1412, 2UPS- IBALL, UNA 600, 4 PRINTERS- HP INKTANK 319, 2 IN NUMBERS CANNON-LJ112E, HP DESKJET 2135, 1 SCANJET PRO 3000 S4 SCANNER, 2 SHARP XEROX MACHINE
12.	PRINCIPAL OFFICE	2 MONITORS- 15" ACER, 15" HP, 1 CPU- ACER ASPIRE, 1 CPU- DELL VOSTRO-3030S, 2 UPS- APC, ZEBRONICS, 1 PRINTER- CANN0N LPP 2900 B
13.	ADMINISTRATIVE OFFICE	1 MONITOR- ACER 15", 1 CPU- ACER VERITON, UPS- HP 600 VA, 1 PRINTER- HP LASERJET P1007
14.	CGHS, ECHS, IVRI & ESIC FACILITY OFFICE AREA	2 MONITORS- 15" ACER, 1 CPU- ACER VERITON, 1 CPU- COMPAQ SG35301L, 2 UPS- MICROTEK, PRO 600, 1 PRINTER- CANN0N LBP 60308, 1 PRINTER- HP INKTANK 319, HP LASERJET MFT 2606
15.	STORE	1 MONITOR- ACER 17", 1 CPU- PRESARIO 2023, UPS- HP 600 VA, 1 PRINTER- HP LASERJET 1020, 1 PRINTER EPSON L3150
16.	LAPTOPS	1 ACER ONE 14Z1, 2 HP COMPAQ PRESARIO C700
17.	TOBACCO CESSATION	1 MONITOR- ACER 15", 1 CPU- ACER VERITON, UPS- HP 600 VA, 1 PRINTER- HP LASERJET 1018

PRINCIPAL OFFICE



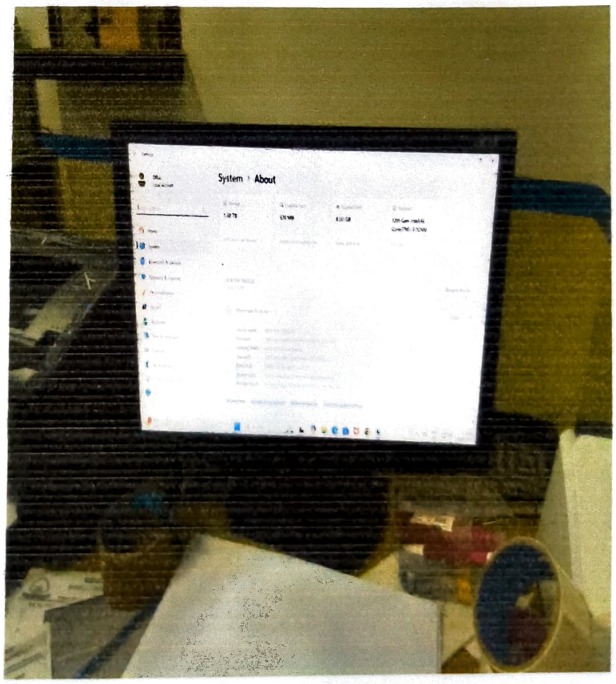
COMPUTER SYSTEM



COMPUTER SYSTEM WITH PRINTER



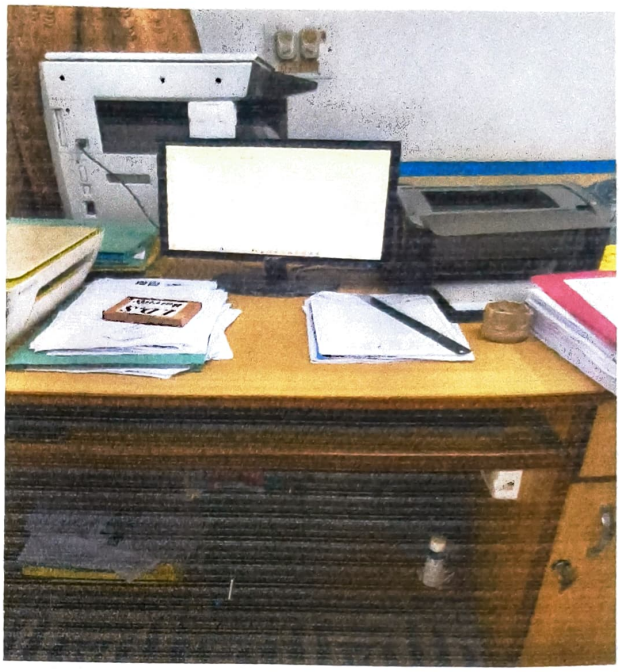
COMPUTER SYSTEM WITH XEROX MACHINE



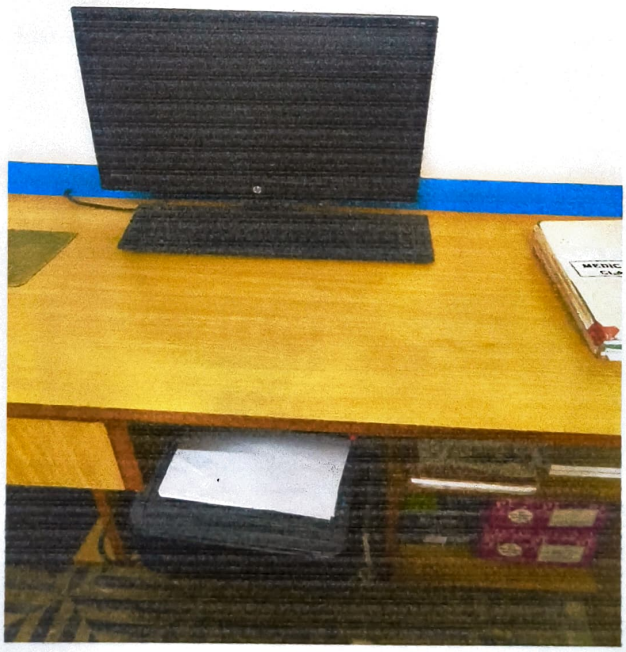
COMPUTER SYSTEM

PRINCIPAL OFFICE





COMPUTER SYSTEM WITH PRINTER & XEROX MACHINE

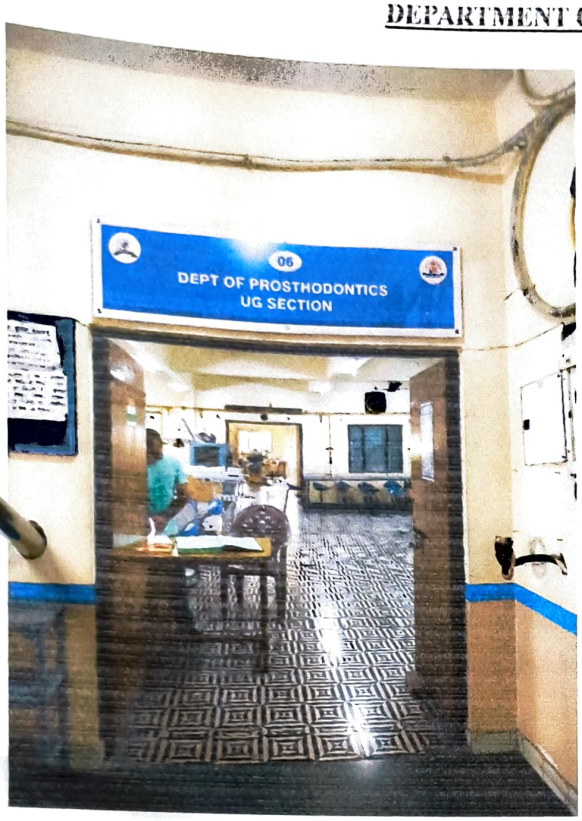


COMPUTER SYSTEM WITH PRINTER

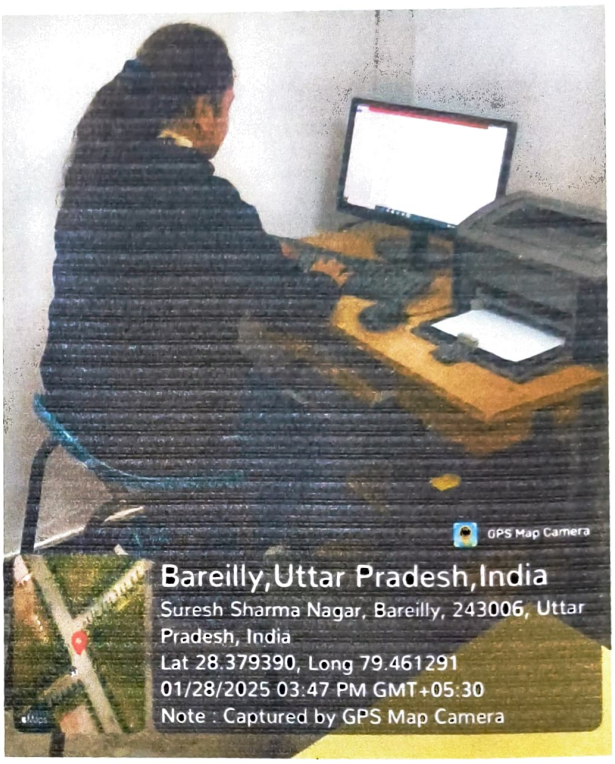
COMPUTER SYSTEM

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pillibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website. www.idsbareilly.in E-mail ID. info@idsbareilly.in Contact No. 0581-2526244

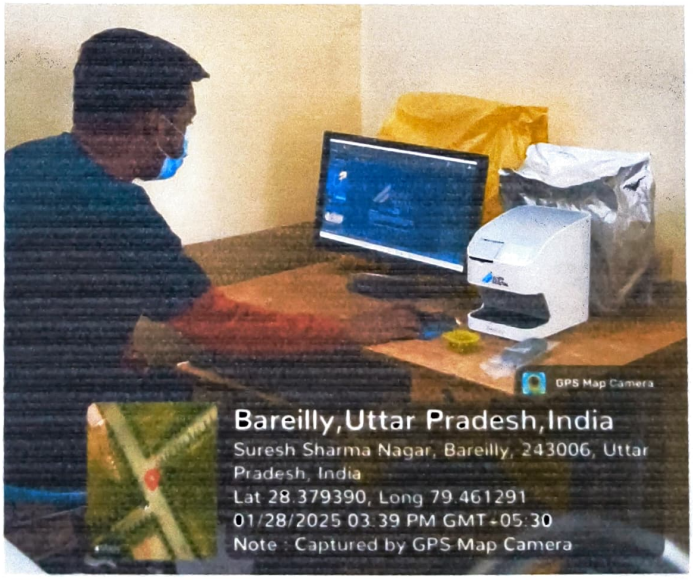
DEPARTMENT OF PROSTHODONTICS



RECEPTION AREA

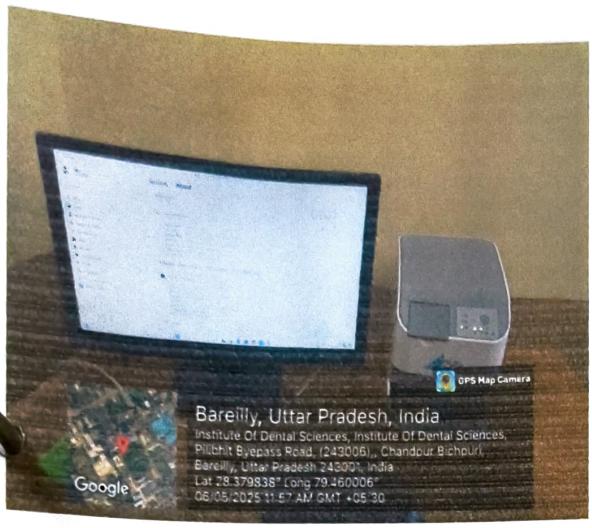


COMPUTER SYSTEM WITH PRINTER



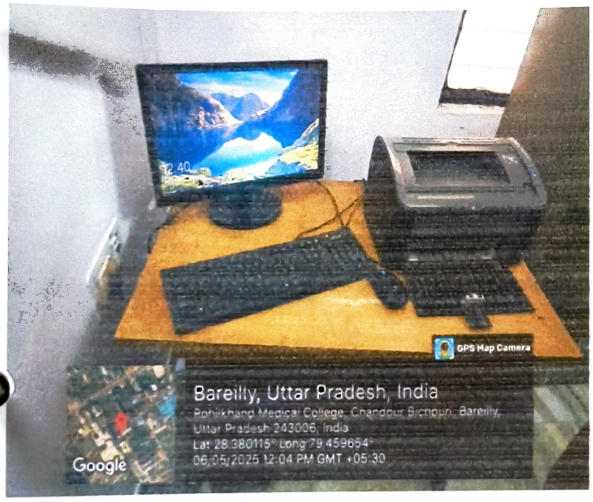
COMPUTER SYSTEM WITH VISTA SCAN FACILITY

DEPARTMENT OF PROSTHODONTICS





COMPUTER SYSTEM WITH VISTA SCAN FACILITY





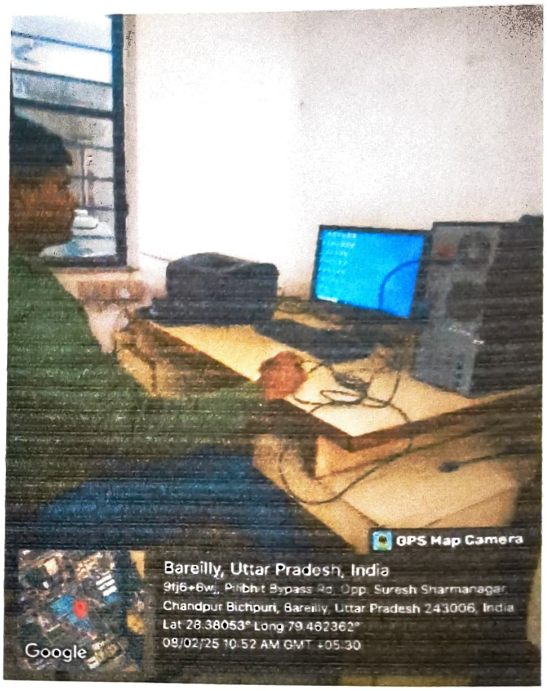
COMPUTER SYSTEM WITH PRINTER

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pillibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website: www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581-2526244

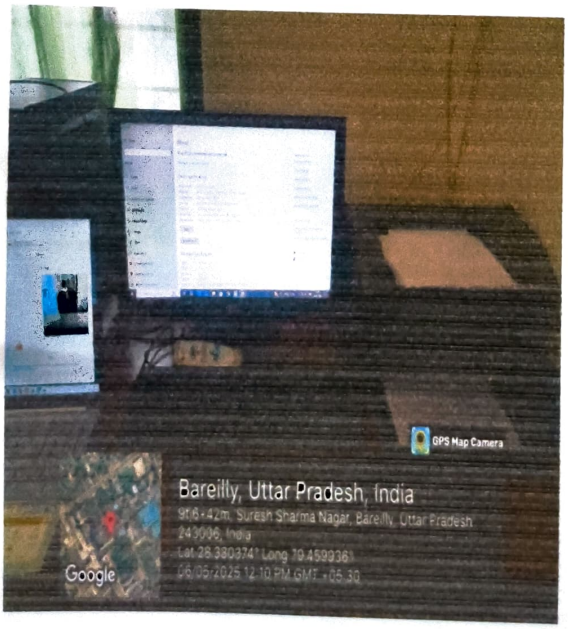
DEPARTMENT OF PUBLIC HEALTH DENTISTRY

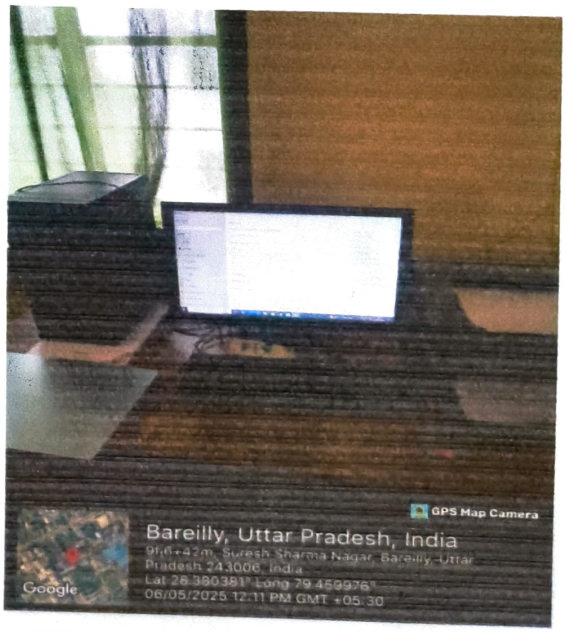


RECEPTION AREA



COMPUTER SYSTEM WITH PRINTER



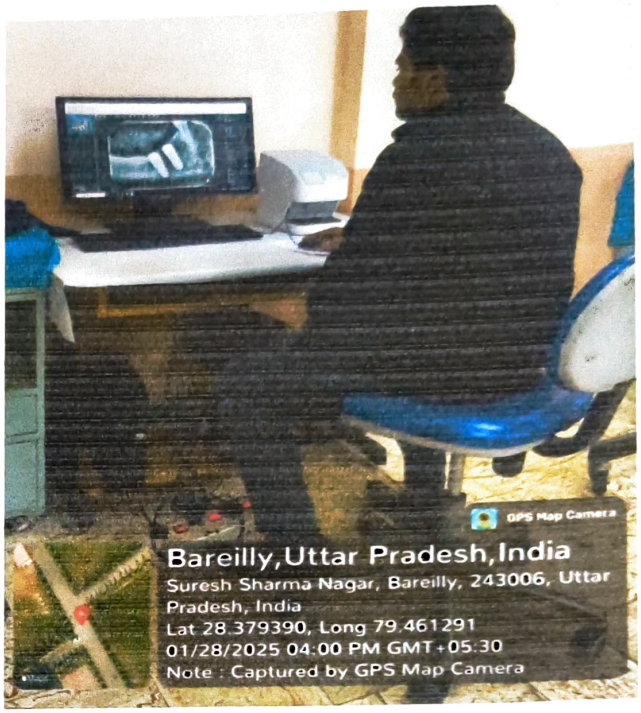


COMPUTER SYSTEM WITH PRINTER

DEPARTMENT OF PERIODONTICS



RECEPTION AREA



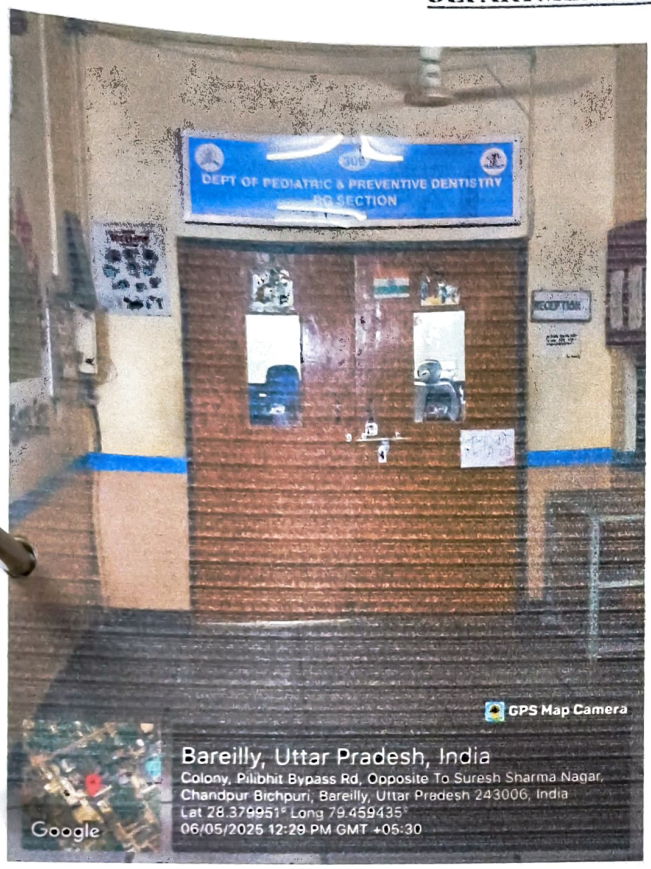
COMPUTER SYSTEM WITH PRINTER

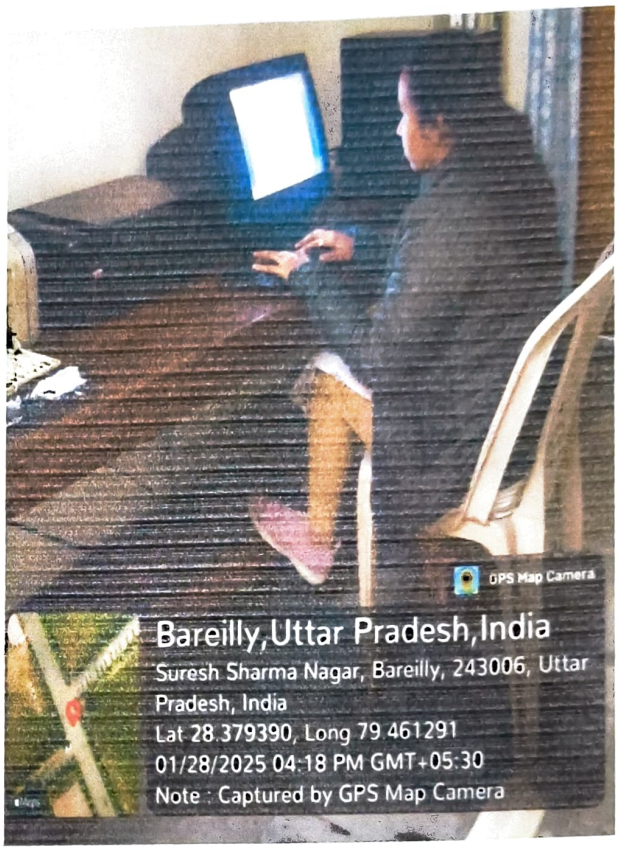


COMPUTER SYSTEM WITH VISTA SCAN

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pilibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website. www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581-2526244

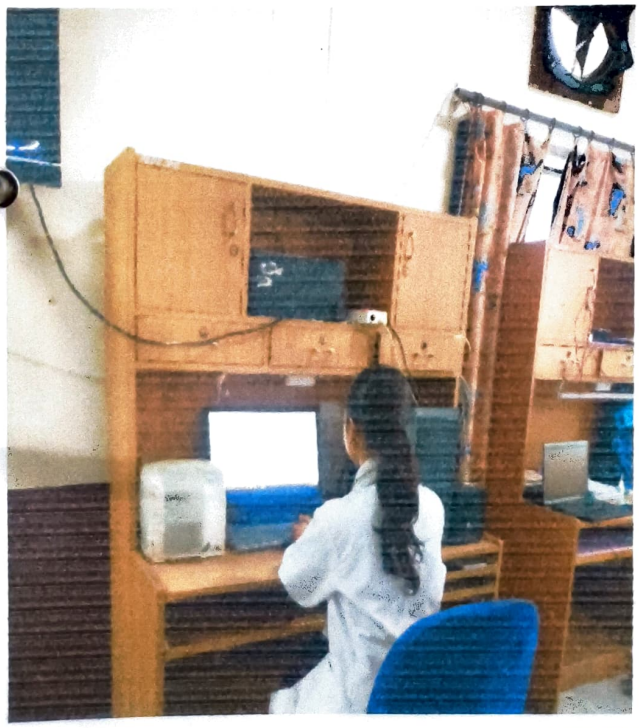
DEPARTMENT OF PEDODONTICS

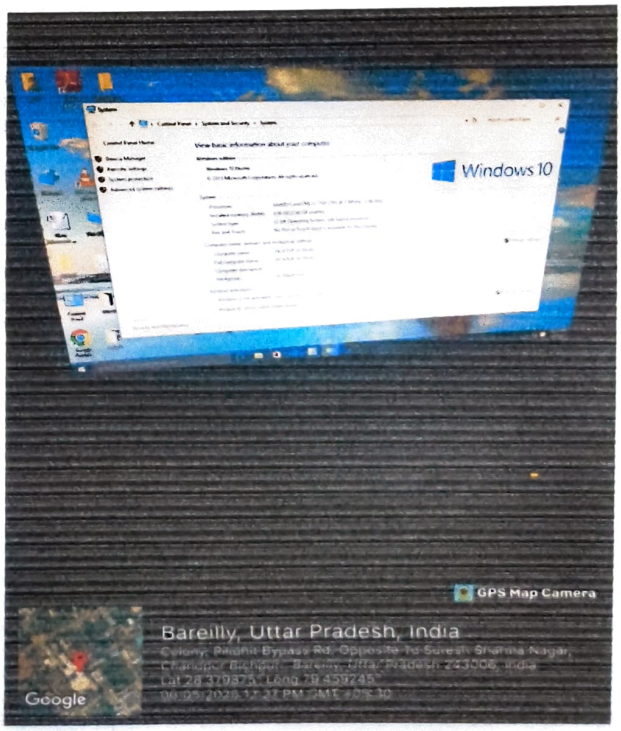




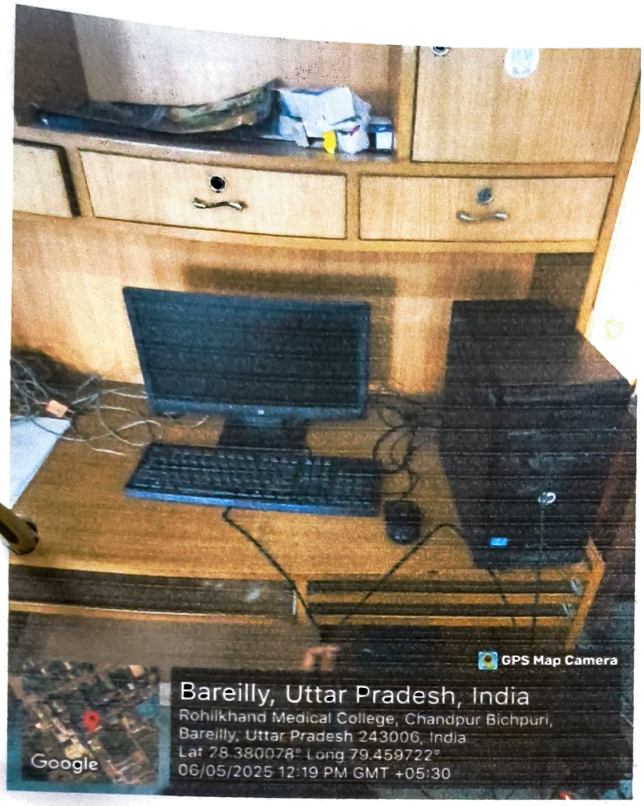
RECEPTION AREA

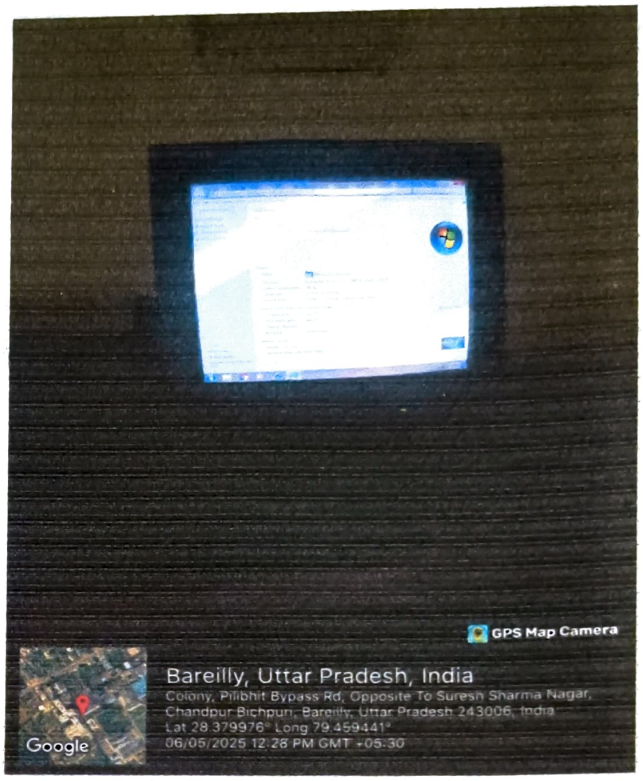
COMPUTER SYSTEM WITH PRINTER





COMPUTER SYSTEM WITH PRINTER





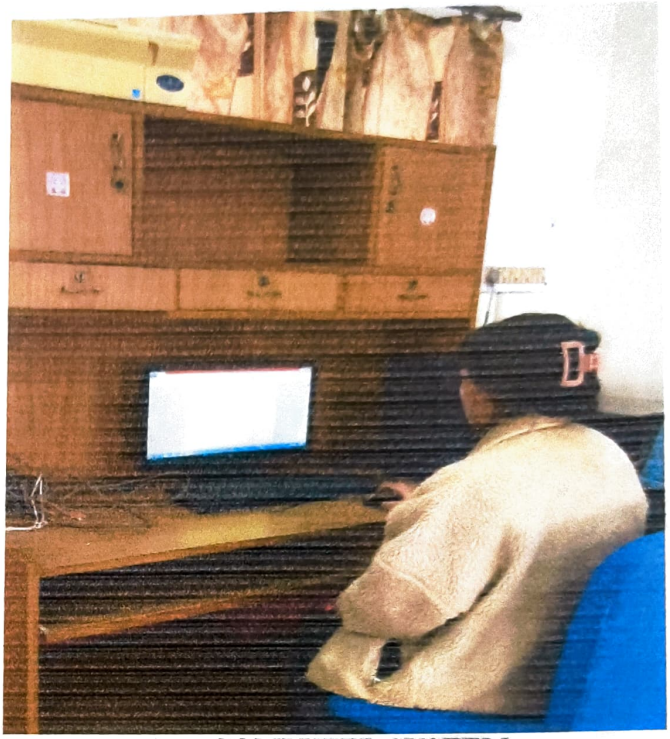
COMPUTER SYSTEM

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pilibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website. www.idsbareilly.in E-mail ID. info@idsbareilly.in Contact No. 0581-2526244

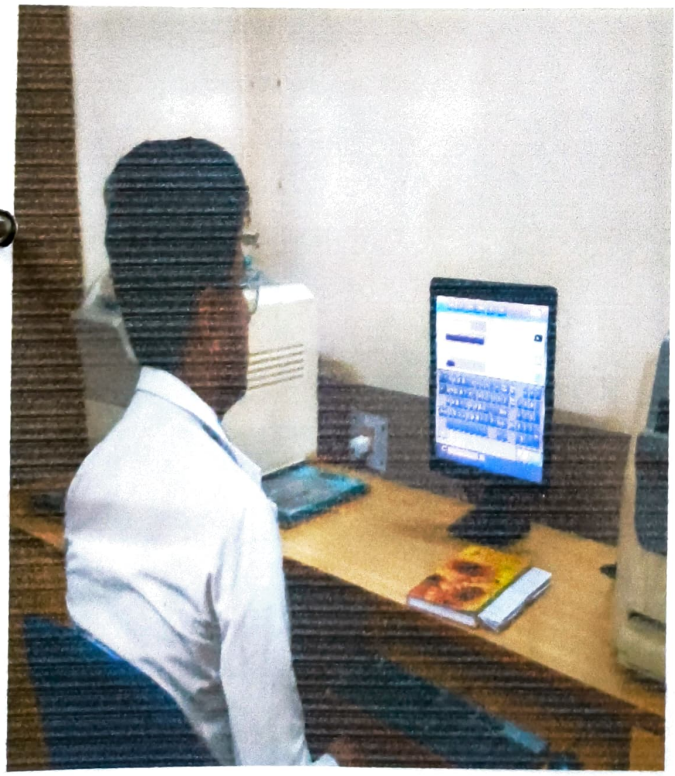
DEPARTMENT OF ORTHODONTICS



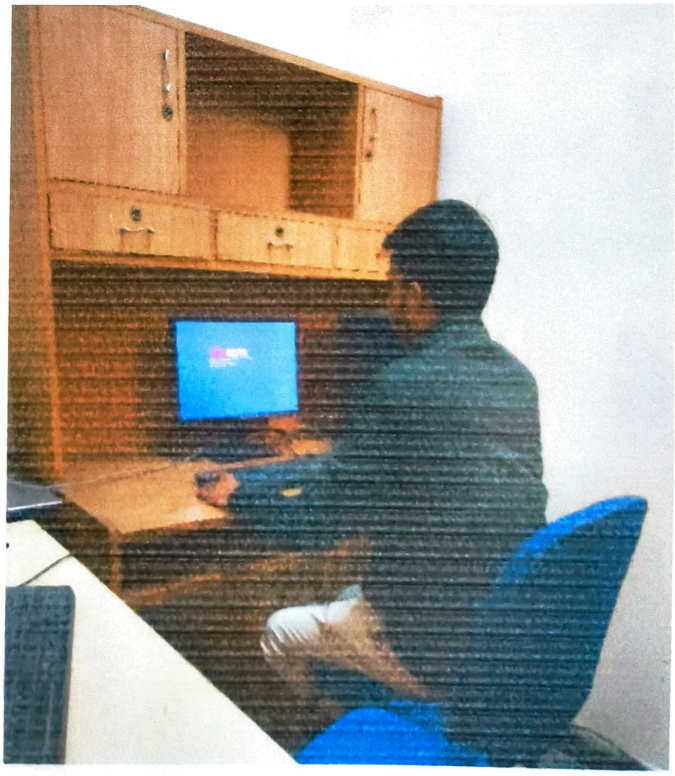
RECEPTION AREA



COMPUTER SYSTEM

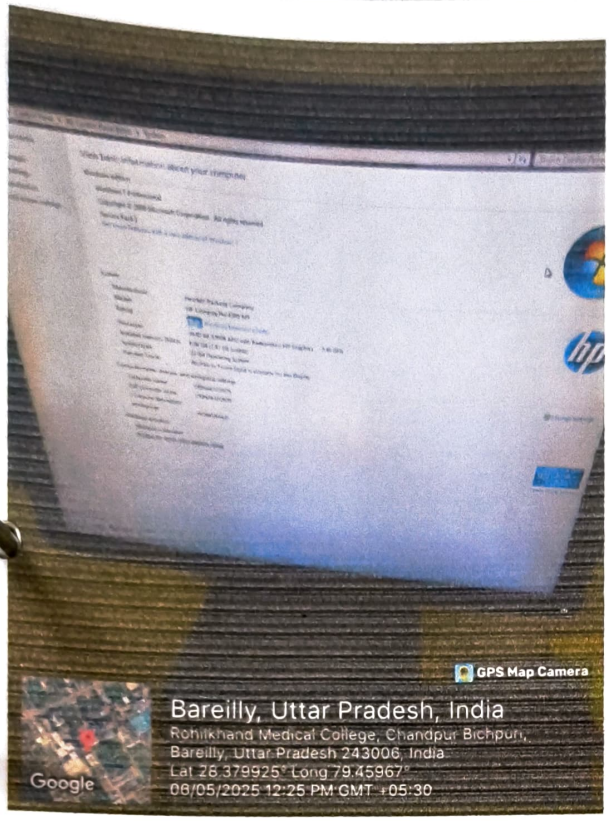


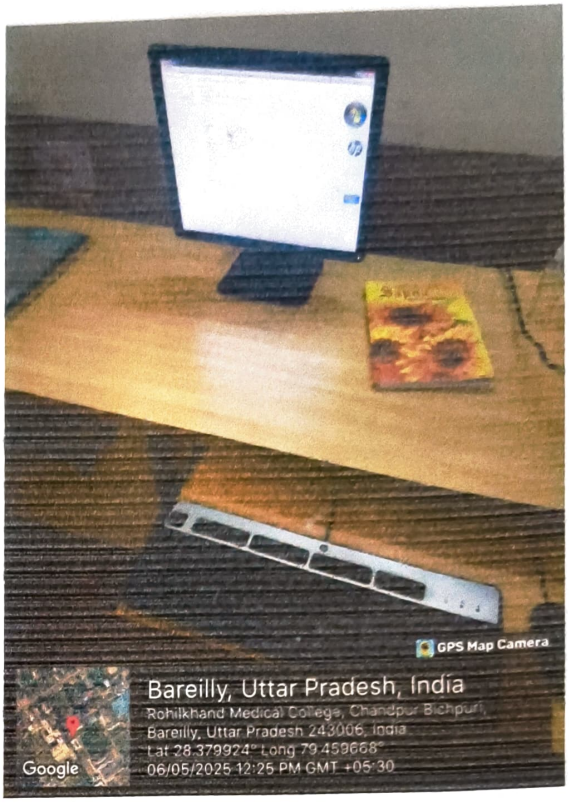
COMPUTER SYSTEM



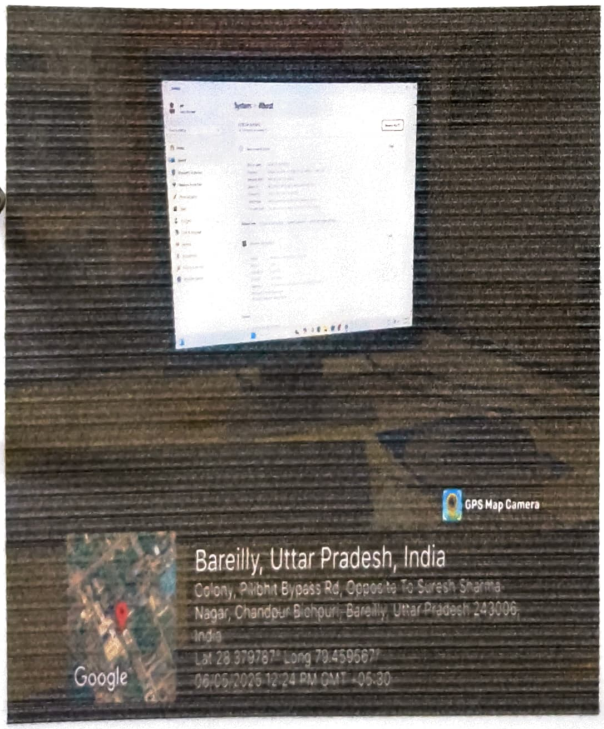
COMPUTER SYSTEM

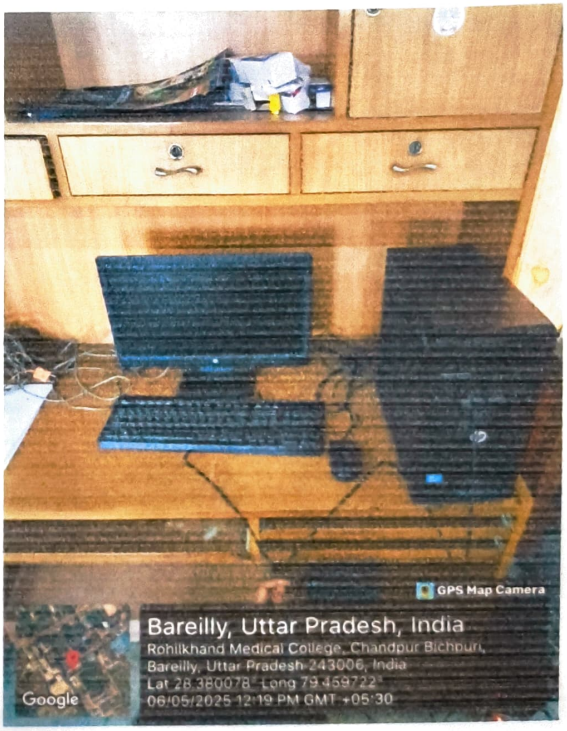
INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pilibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website. www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581-2526244





COMPUTER SYSTEM

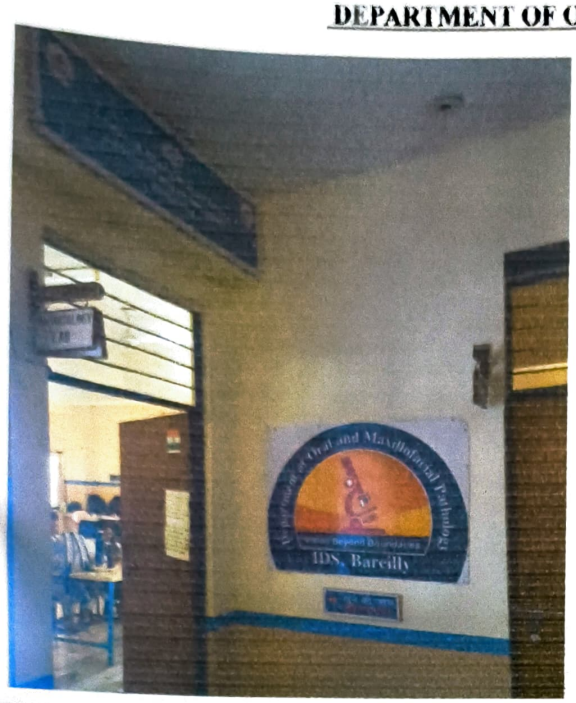




COMPUTER SYSTEM

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pilibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website: www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581-2526244

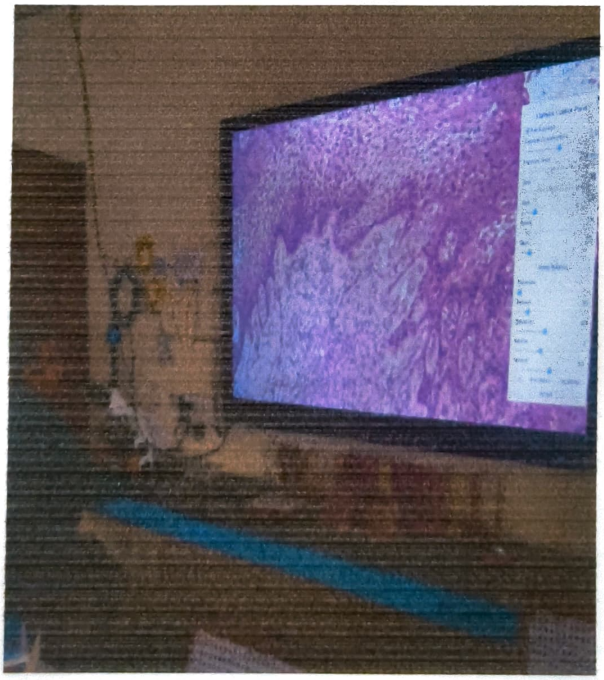
DEPARTMENT OF ORAL PATHOLOGY



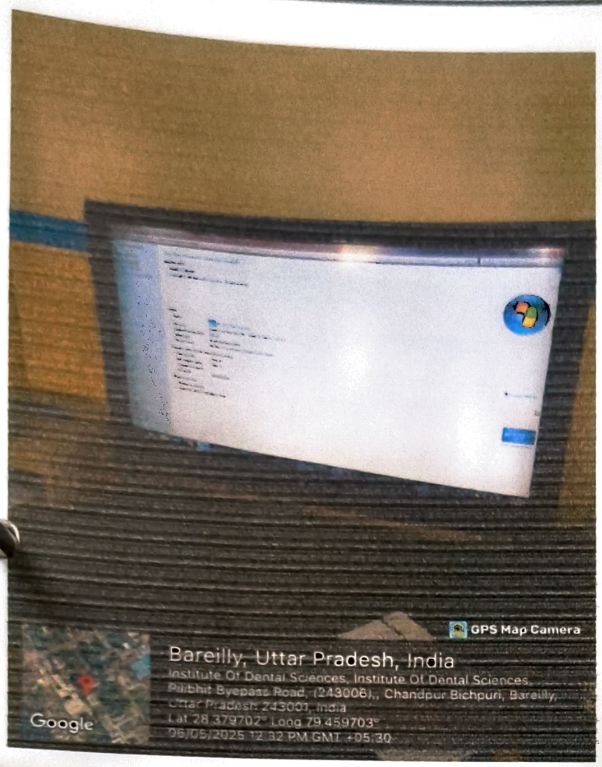
RECEPTION AREA



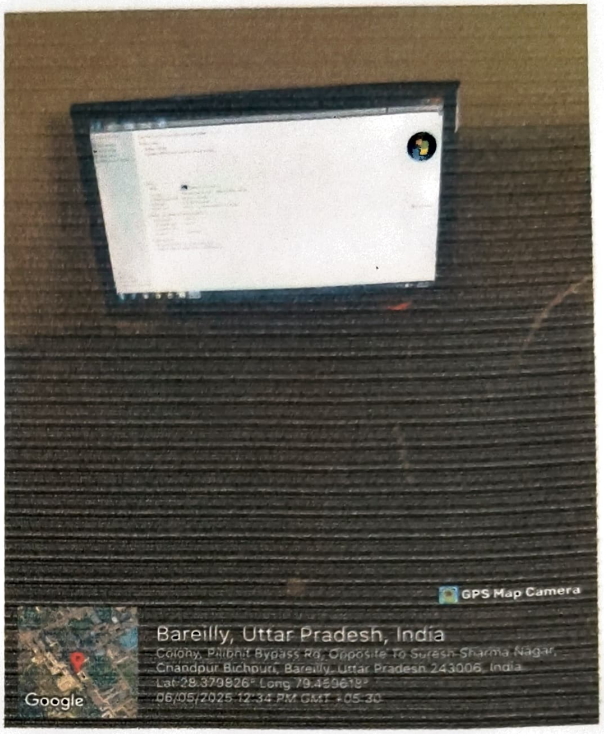
COMPUTER SYSTEM WITH PRINTER



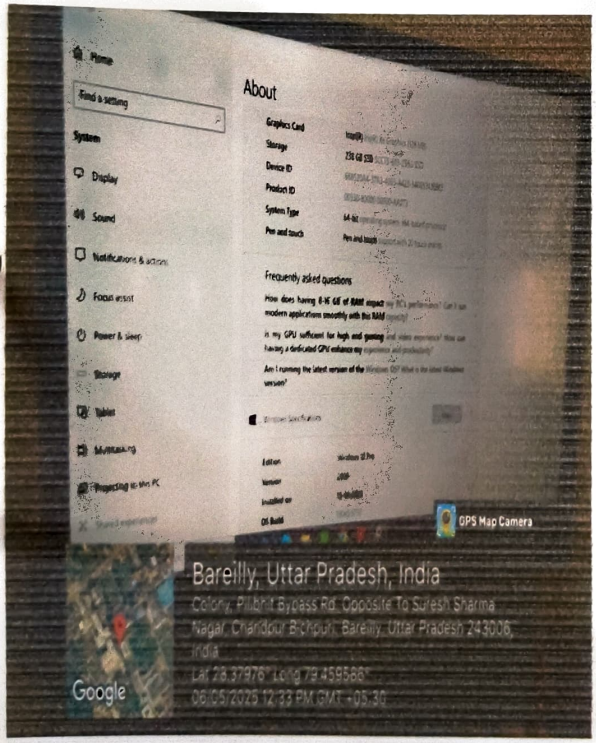
SMART BOARD FACILITY WITH WI–FI CONNECTIVITY



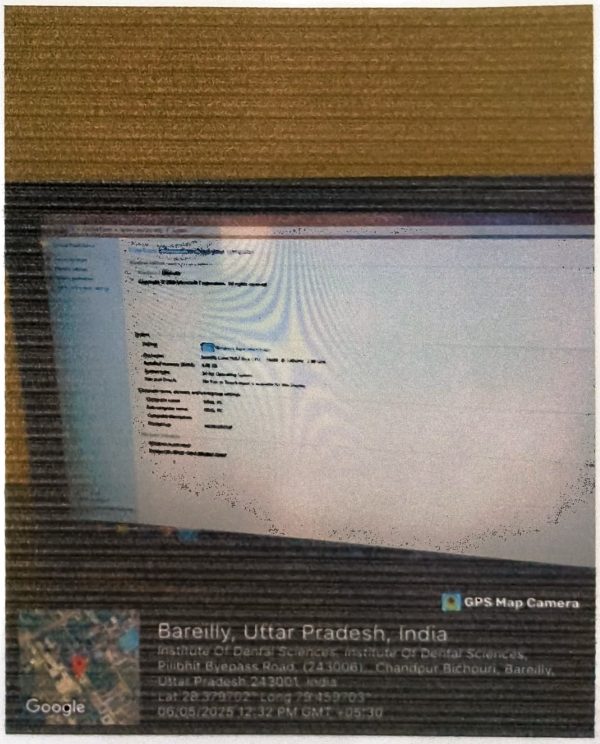
COMPUTER SYSTEM



COMPUTER SYSTEM



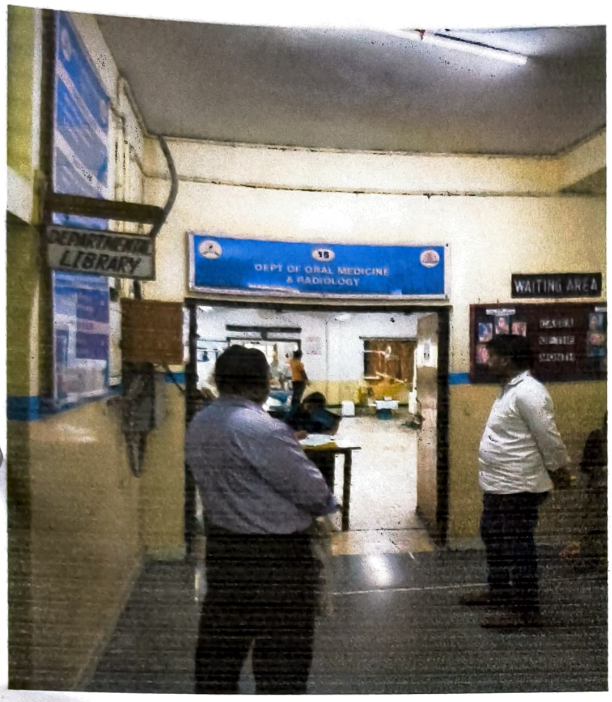
COMPUTER SYSTEM



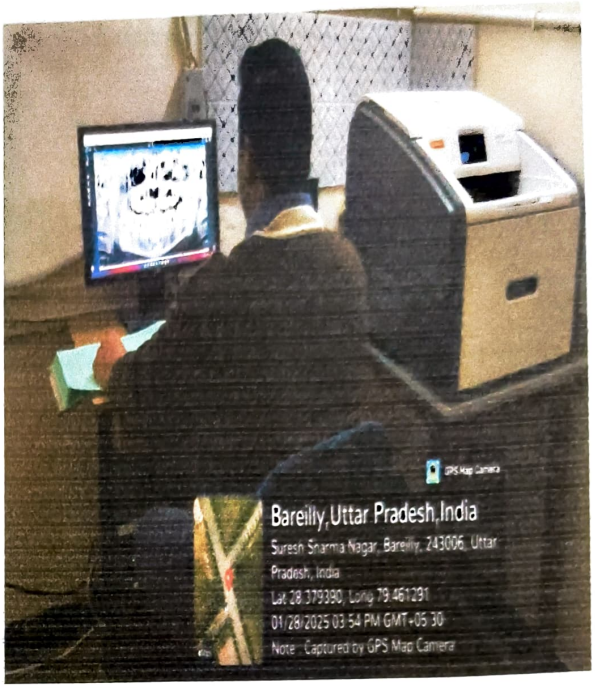
COMPUTER SYSTEM

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pillibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website: www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581-2526244

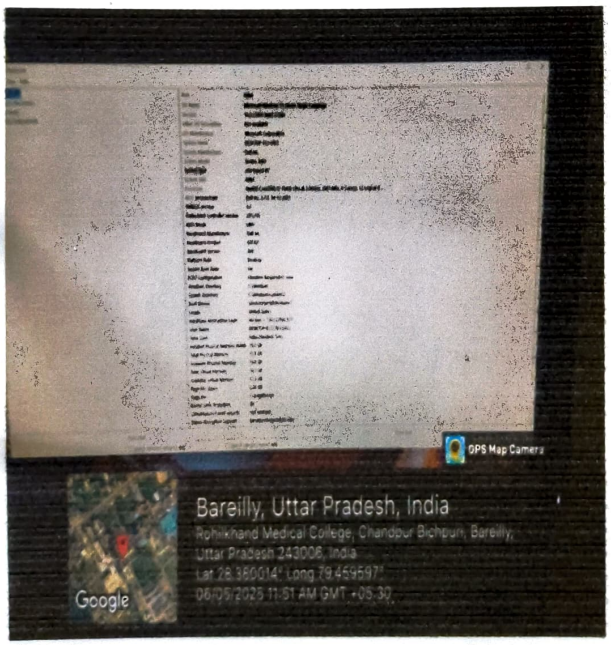
DEPARTMENT OF ORAL MEDICINE & RADIOLOGY



RECEPTION AREA



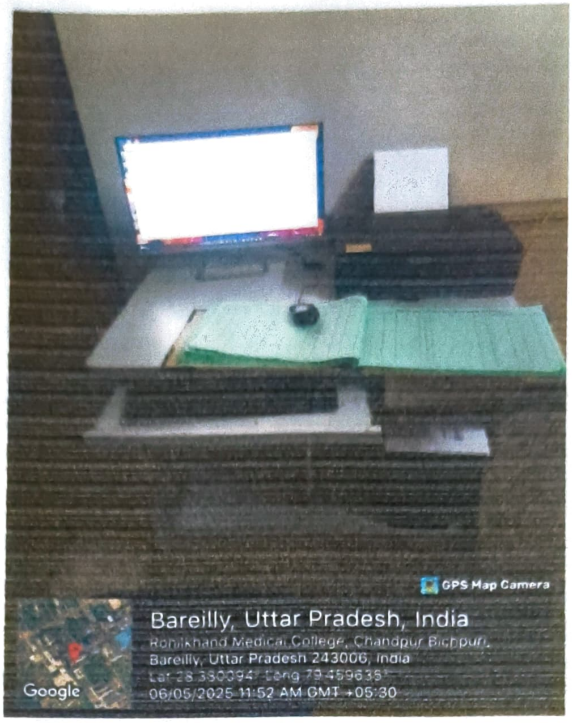
COMPUTER SYSTEM FOR OPG WITH PRINTING FACILITY



COMPUTER SYSTEM



COMPUTER SYSTEM WITH VISTA SCAN FACILITY



COMPUTER SYSTEM WITH PRINTER FACILITY

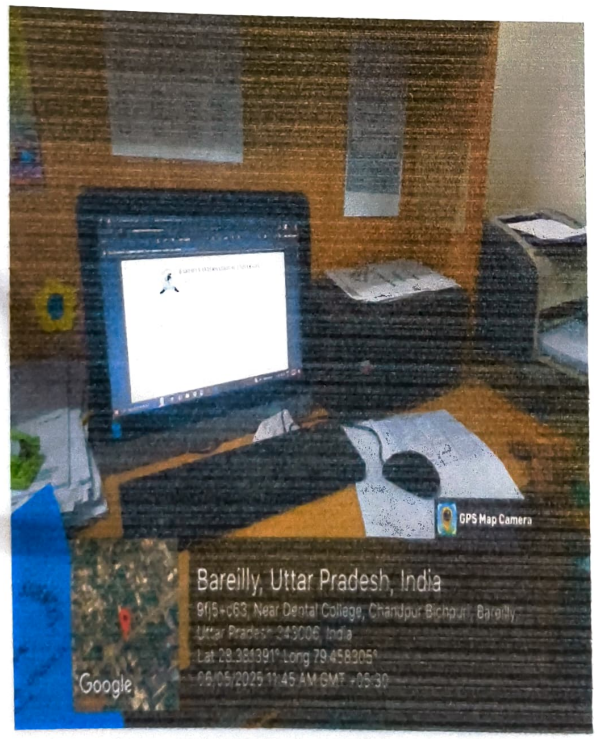
DEPARTMENT OF CONSERVATIVE & ENDODONTICS



RECEPTION AREA



COMPUTER SYSTEM WITH VISTA SCAN



COMPUTER SYSTEM WITH PRINTER



COMPUTER SYSTEM WITH VISTA SCAN



COMPUTER SYSTEM WITH PRINTER FACILITY

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pilibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website: www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581 2526244

DEPARTMENT OF ORAL AND MAXILLOFACIAL SURGERY



RECEPTION AREA



COMPUTER SYSTEM

WITH VISTA SCAN



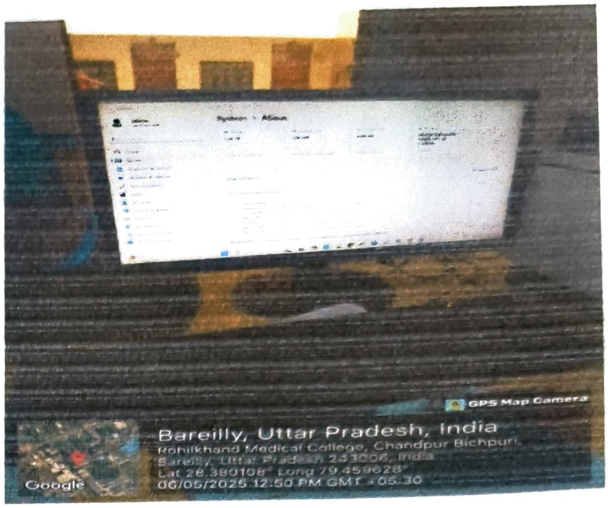


COMPUTER SYSTEM WITH PRINTER FACILITY

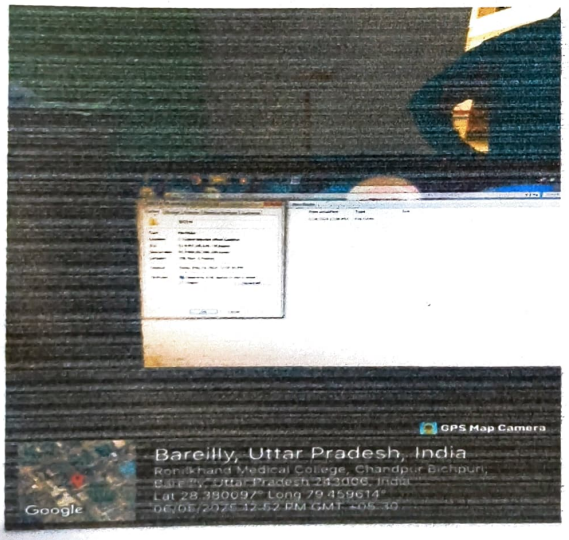
CGHS, ECHS, IVRI & ESIC FACILITY OFFICE AREA



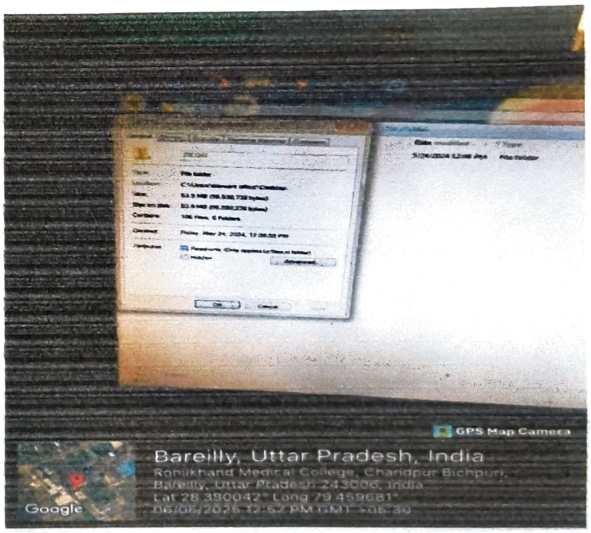
RECEPTION AREA



COMPUTER SYSTEM

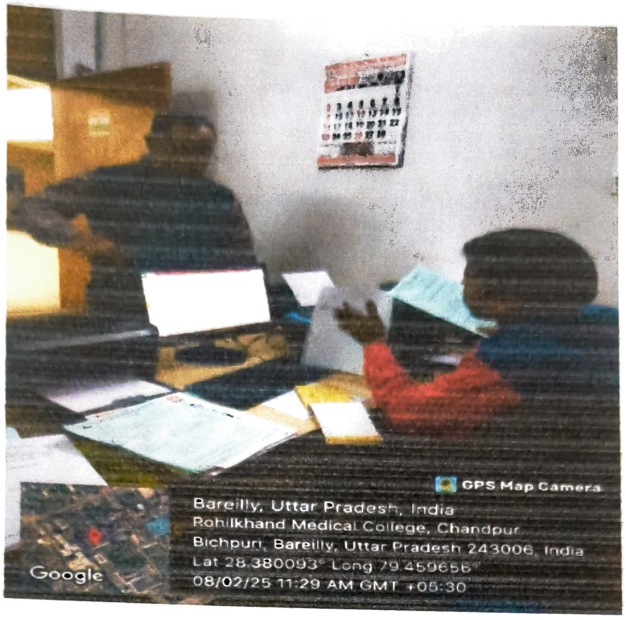


COMPUTER SYSTEM



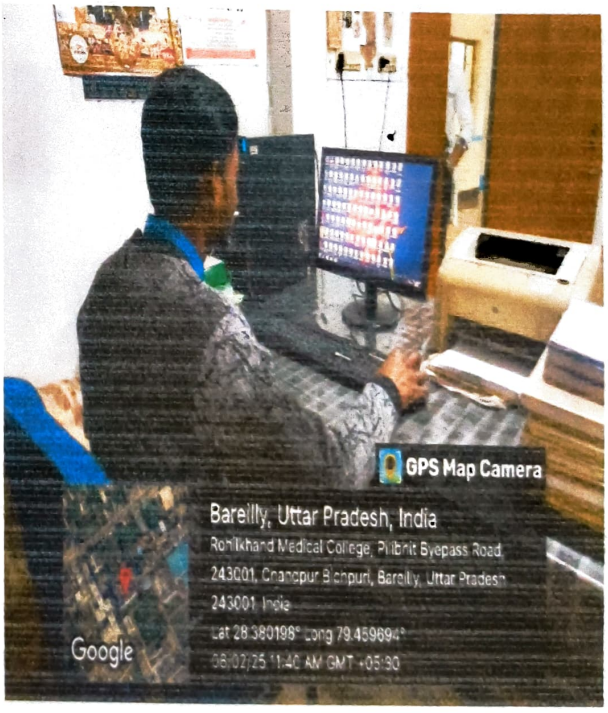
COMPUTER SYSTEM

CGHS, ECHS, IVRI & ESIC FACILITY OFFICE AREA



COMPUTER SYSTEM WITH PRINTER



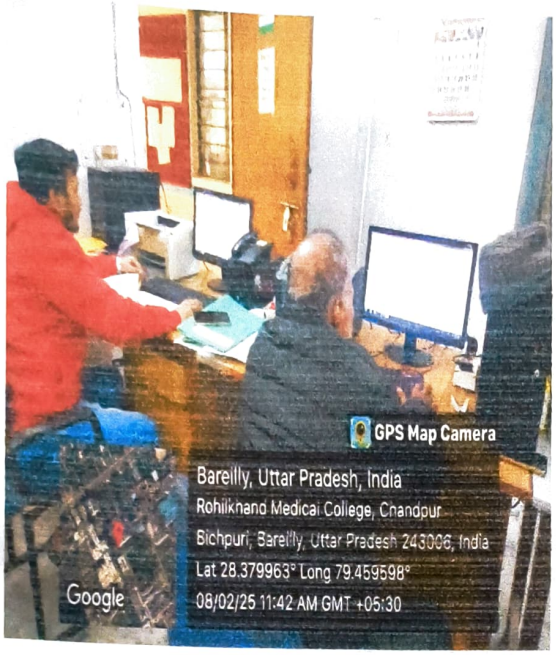


TABACCO CAESSATION CENTRE

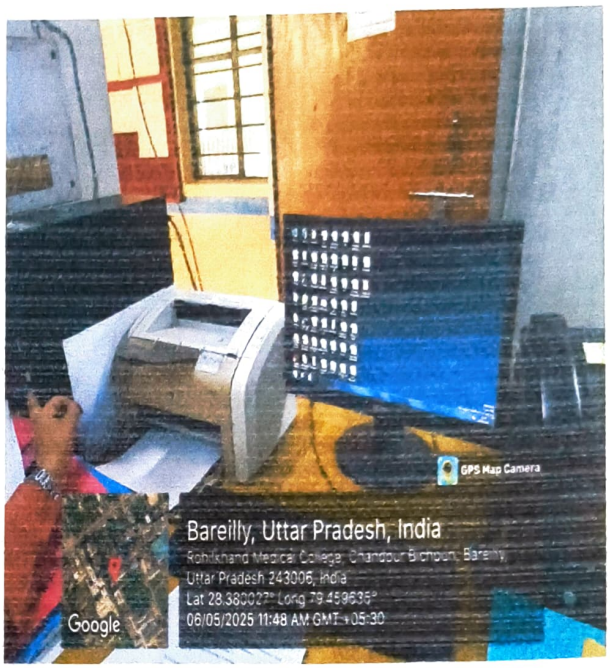
DENTAL STORE

INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pillibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website: www.idsbareilly.in E mail ID: info@idsbareilly.in Contact No. 0581 2526244

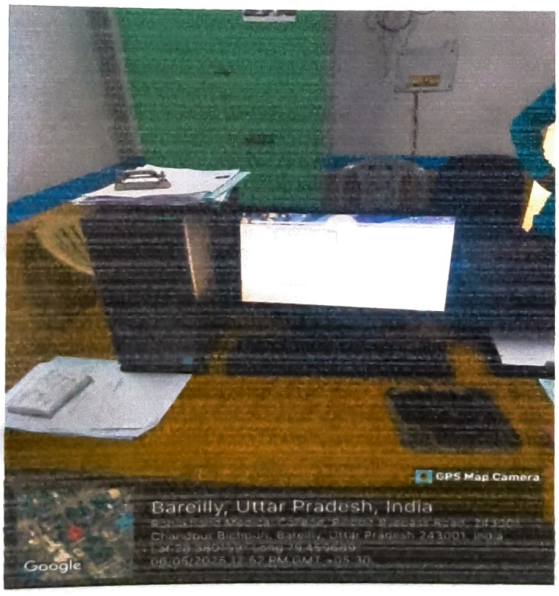
EXAMINATION CELL OFFICE



RECEPTION AREA



COMPUTER SYSTEM WITH PRINTER



COMPUTER SYSTEM

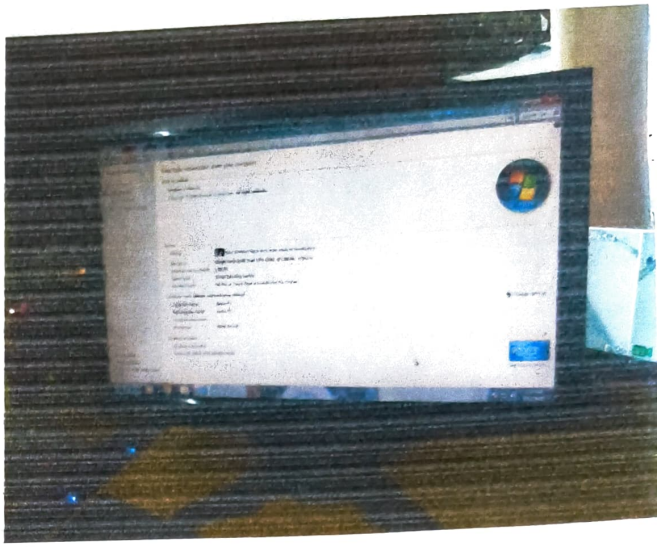


COMPUTER SYSTEM WITH PRINTER

ADMINISTRATIVE OFFICER ROOM



CCTV MONITERING UNIT



COMPUTER SYSTEM

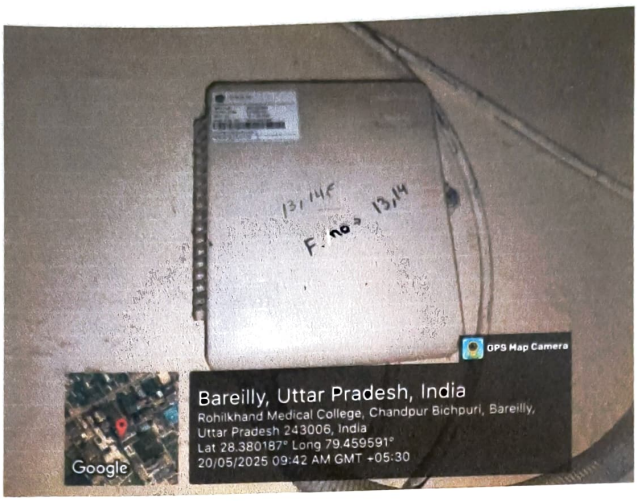
INSTITUTE OF DENTAL SCIENCES
BAREILLY INTERNATIONAL UNIVERSITY, BAREILLY
Pillibhit By Pass Road, Bareilly-(U.P.) 243006, INDIA
Website: www.idsbareilly.in E-mail ID: info@idsbareilly.in Contact No. 0581-2526244

List of Wifi Access Points

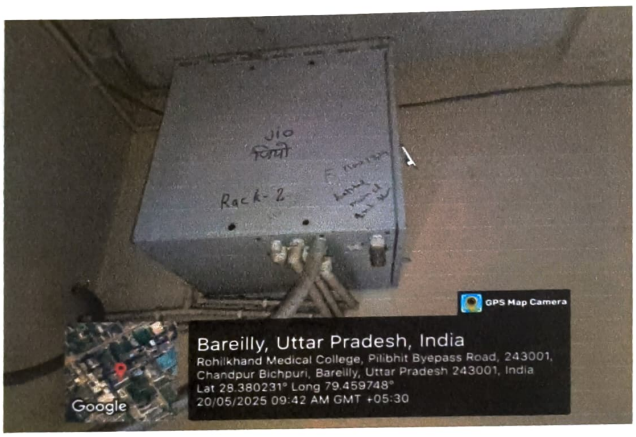
Principle office	1
Reception	1
Oral Pathology	1

4.4.2

Wi Fi Points



PRINCIPAL OFFICE



RECEPTION

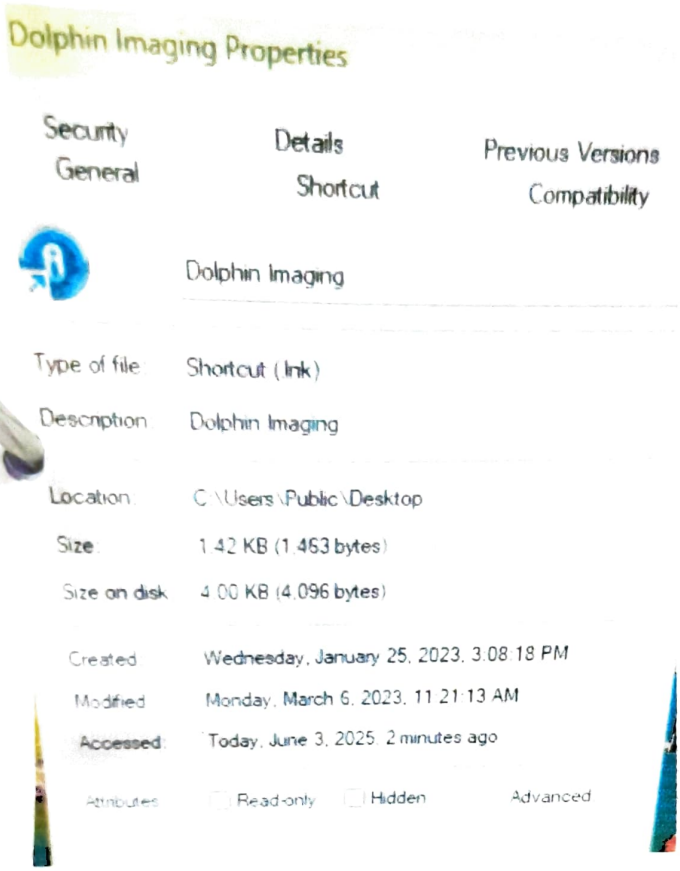


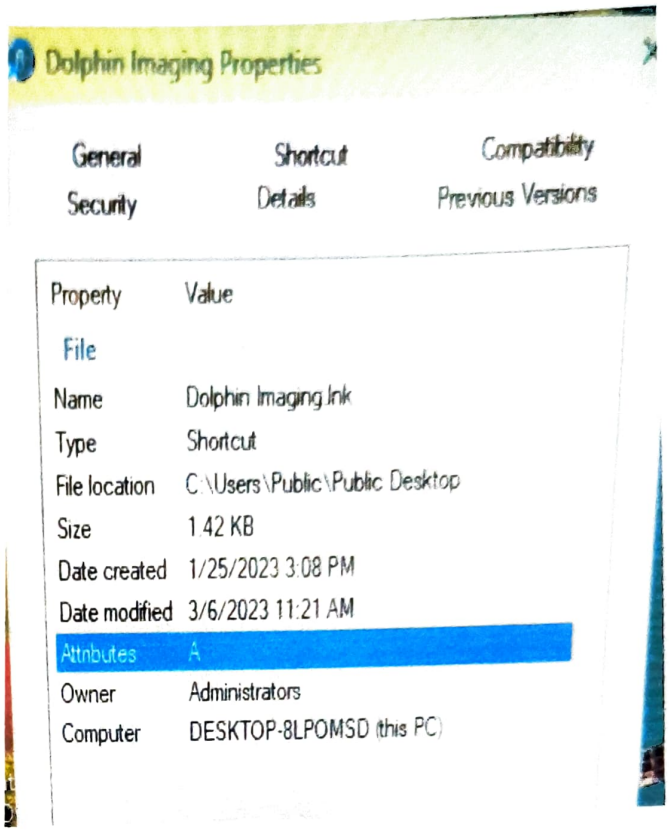
ORAL PATHOLOGY AREA

List of Open Source Softwares

Dolphin Imaging	1
Vista Scan	5
Carestream	1
VAtech	1
Image analysis software	1
Moticam software	1

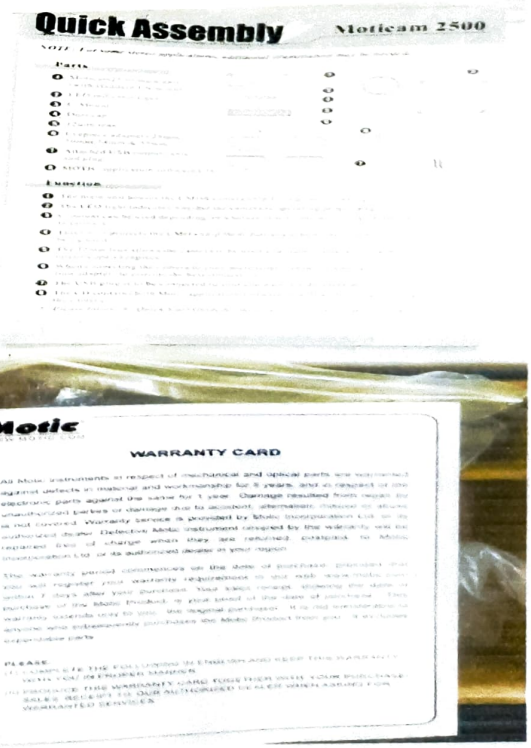
4.4.2





Detail of Dolphin imaging software in Orthodontic department

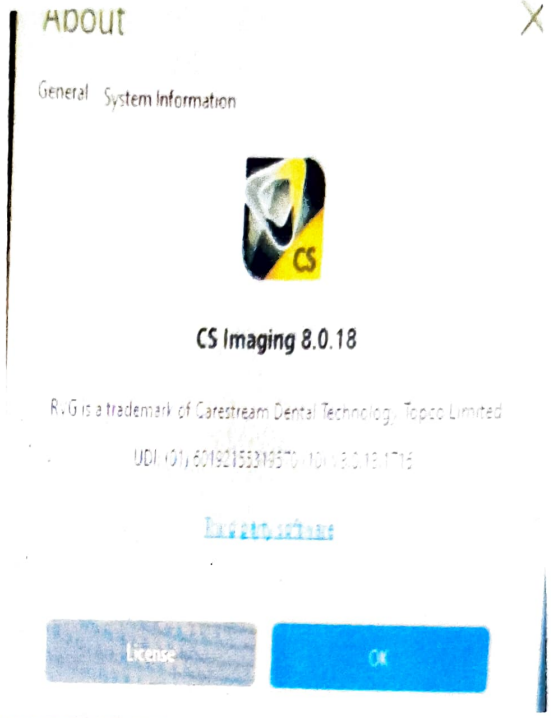




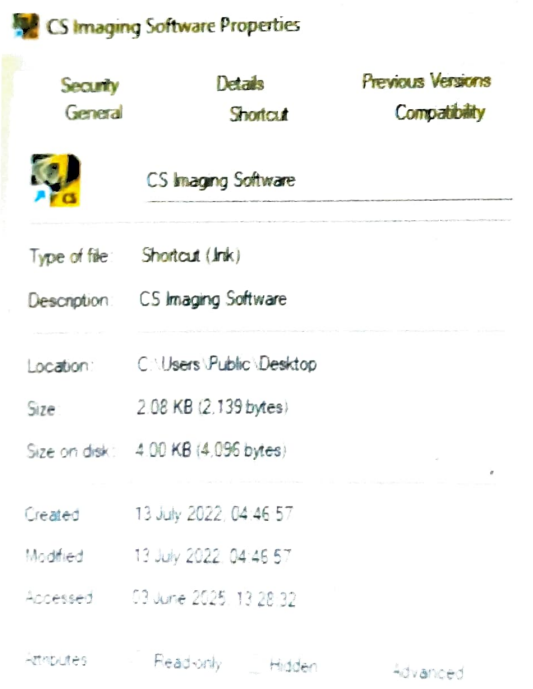
Moticam Software used in Oral pathology



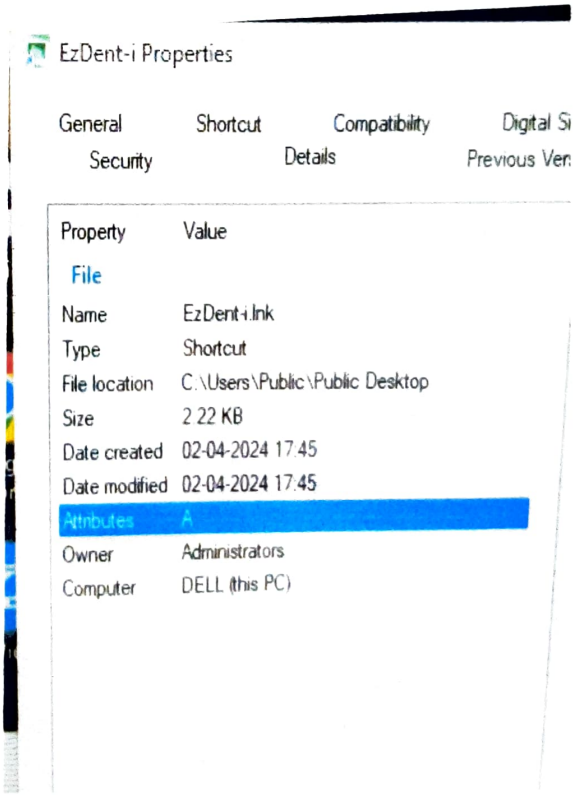
Image analysis software in OP



Carestream Software in OMDR

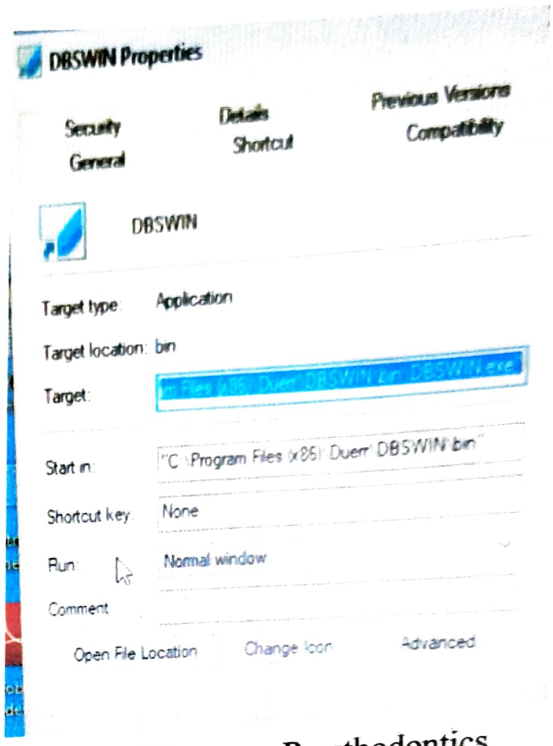


Carestream in OMDR



VATECH in OMDR for CBCT





VISTA scan software used in Endodontics, Oral Surgery, Prosthodontics, Pedodontics, Periodontics

Information Technology (IT) Policy

Introduction:

Institute of Dental Sciences recognizes Information Technology (IT) as a strategic asset integral to achieving academic excellence, operational efficiency, and institutional innovation. The Institution's IT Policy is established to ensure optimal utilization of digital resources, enhance data security, promote digital literacy, and comply with national and international cyber regulations.

Key Objectives:

1. **Regulating Use of IT Resources**: Establish clear guidelines and responsibilities to ensure appropriate and effective use of the Institution's IT infrastructure.
2. **Data Security**: Implement stringent access controls and encryption protocols to protect institutional data and personal information from unauthorized access, breaches, or misuse.
3. **Legal Compliance**: Ensure all software, hardware, and digital platforms comply with national laws, licensing norms, and international standards related to data protection and digital rights.
4. **Investment in Technology**: Promote cost-effective and scalable IT investments that align with the Institution's strategic goals, academic priorities, and operational requirements.
5. **Digital Literacy and Capacity Building**: Enhance the digital competencies of students, faculty, and staff through continuous training, user support services, and awareness programs.
6. **Sustainability and Green IT**: Encourage environmentally conscious computing practices, including the use of energy-efficient devices, virtualization, and responsible e-waste disposal.

7. **Research and Collaboration**: Foster academic innovation and enhance global research visibility through the development of an Institutional Repository and collaborative technology
8. **Governance and Accountability**: Establish a transparent and accountable governance structure for managing IT resources and addressing disputes or policy violations.

Roles and Responsibilities:

At Institute of Dental Sciences, the IT Policy assigns specific responsibilities to various stakeholders to ensure effective governance of digital resources. The IT Department manages infrastructure, cyber security, and user support. Faculty members are expected to promote ethical digital practices and guide students in responsible technology use. Students must adhere to usage guidelines and maintain data confidentiality. Administrative staff are responsible for secure handling of institutional data, while research scholars must comply with ethical standards in digital research. External vendors are required to follow strict data protection protocols during their engagement with the Institution.

IT Hardware Installation Policy:

Procurement and Approval: All IT hardware must be procured through a centralized system managed by the Institution's IT Department Hardware requests must be justified through need-based proposals submitted by department heads. Approval must be obtained from the Finance and IT Committees before any procurement is initiated.

Installation Standards: Only IT Department personnel or authorized service providers are permitted to install or configure hardware on Institution premises. All installed hardware must be registered in the Institution's digital asset inventory and labelled with an official asset tag.

Compatibility and Integration: New hardware must be compatible with the existing network infrastructure, software ecosystem, and power supply.

Security Considerations: Any hardware device that connects to the Institution network must comply with security policies, including endpoint protection, firmware validation, and port access control. Unauthorized modification, tampering, or relocation of installed hardware without IT Department consent is strictly prohibited.

Maintenance and Support: Routine preventive maintenance schedules will be maintained for critical infrastructure, including servers and routers. Users must report malfunctioning or damaged equipment to the IT helpdesk for inspection and service.

Disposal and Replacement: Hardware deemed obsolete or irreparable must be retired following the Institution's e-waste disposal guidelines. Replacement requests must be supported with performance reports and approval from designated committees.

Audit and Compliance: Periodic audits will be conducted to verify the location, condition, and usage of IT hardware. This policy ensures that 's IT infrastructure remains secure, efficient, and aligned with the Institution's academic and administrative objectives

Software Installation and Licensing Policy:

Institute of Dental Sciences Software Installation and Licensing Policy ensures ethical, secure, and compliant use of software across its campuses. All software must be procured through the IT Department, with a preference for licensed, open-source, or institutionally approved applications. Only authorized IT personnel are permitted to install software, following a formal request and approval process. Users are prohibited from installing unauthorized software or sharing licensed applications externally. Regular audits are conducted to maintain compliance, and violations may result in disciplinary actions.

Use of IT Devices on Network:

Institute of Dental Sciences () has established a comprehensive policy governing the use of IT devices on its network to ensure security, compliance, and optimal performance. All personal and institutional devices must be registered with the IT Department, tagged with a unique user ID and MAC address, and meet security standards including updated antivirus software and strong passwords. Personal devices (BYOD) require IT approval and configuration before accessing the Institution Wi-Fi, with users agreeing to periodic security scans and audits. Acceptable use is limited to official academic and administrative activities; activities like streaming, torrenting, and gaming are prohibited. The IT Department monitors all network activity, and violations may result in disconnection or disciplinary action. During online assessments, only Institution-provided devices are permitted unless explicitly approved.

Desktop Devices:

Institute of Dental Sciences (IDS) has implemented a comprehensive Desktop Devices Policy to ensure secure, efficient, and standardized use of desktop computers across its campuses. This policy governs the allocation, setup, authorized use, security measures, maintenance, software usage, data storage, energy efficiency, and disposal of desktop systems. Key provisions include:

- **Allocation and Setup:**

- **Authorized Use:**
- **Security Measures:**
- **Maintenance and Repairs:**
- **Data Storage and Backup:**
- **Disposal and Replacement:**

Use of Portable Devices:

The Use of Portable Devices Policy at Institute of Dental Sciences () regulates the access, security, and permissible use of mobile and portable digital devices within the Institution ecosystem. This policy ensures the protection of Institution data while supporting flexibility and remote access. Portable devices include laptops, tablets, smartphones, USB drives, external hard disks, and any wearable or handheld digital equipment. Students, faculty, researchers, and staff may use approved portable devices for academic and administrative purposes. Devices may connect to Institution Wi-Fi and intranet services upon registration and security clearance by the IT Department. All devices must be registered with the IT Department, and users must provide device details (model, OS, MAC address, serial number). Personal devices accessing sensitive Institution data must be enrolled in the Mobile Device Management (MDM) system if applicable. Devices must have up-to-date antivirus protection, encrypted storage, and secure access protocols (passwords, PINs, biometric authentication).

Devices should be configured to auto-loek when inactive and be capable of remote data wipe in case of loss or theft. Confidential or sensitive Institution data must not be stored unencrypted on portable devices. Any data copied to portable storage (e.g., USB drives) must be temporary and backed up to the Institution's secure network within 24 hours. Jail broken or rooted devices are not permitted to connect to the Institution network. Portable devices must not be used to transmit pirated content, install unauthorized software, or access restricted sites. Devices should not be connected to projectors, display units, or labs without permission from the lab supervisor or IT staff. Users must report any loss or theft of portable devices used for Institution purposes within 24 hours to the IT Department and, if applicable, local authorities. The IT Department will take necessary steps to disable access or initiate remote data deletion. reserves the right to audit portable device configurations, monitor access logs, and enforce data protection compliance for registered devices.

Breach of This Policy:

The Breach of IT Policy at Institute of Dental Sciences outlines the consequences and corrective measures for violations of the institution's IT guidelines. A breach occurs when an individual or group deliberately or unintentionally violates any clause of the IT policy, including unauthorized access, data theft, malware distribution, installation of pirated software, network misuse, and failure to report security incidents. Violations are categorized into minor, moderate, and major breaches, each with corresponding disciplinary actions ranging from warnings and mandatory training to permanent revocation of IT access and legal action under applicable Indian laws. All suspected breaches must be reported immediately to the IT Department or the designated Cyber security Officer through secure internal channels, ensuring confidentiality for whistle blowers. The IT Department conducts preliminary inquiries followed by formal investigations in consultation with legal and administrative units, during which temporary suspension of access privileges may be imposed. Disciplinary measures align with Institution policies, employment contracts, and student codes of conduct, potentially involving HR intervention, suspension, termination, academic sanctions, or suspension from Institution programs. Severe violations may be referred to law enforcement agencies and prosecuted under relevant laws, including the Information Technology Act, 2000. Access may be reinstated only upon completion of disciplinary procedures and implementation of corrective action plans, with recurrent breaches potentially leading to permanent denial of access. To prevent breaches, conducts regular awareness programs, cyber security drills, and mandatory training sessions, and deploys automated monitoring tools to detect anomalies and alert administrators in real time.

PRINCIPAL

Date:

Place:

Table of Contents

1. Abbreviations 2
2. Introduction 2
3. Scope 3
4. Objective 3
5. Roles and Responsibilities 4
6. Acceptable Use 5
7. IT Hardware Installation Policy 6
8. Software Installation and Licensing Policy 7
9. Use of IT Devices on BIU Network 8
10. Desktop Devices 9
11. Sharing of Data 11
12. Use of Portable Devices 12
13. Network (Intranet & Internet) Use Policy 13
14. Email Account Usage Policy 15
15. Institutional Repository (IR) 16
16. Disposal of ICT Equipment 17
17. Budgetary Provisions for ICT 19
18. Breach of This Policy 20
19. Revisions to Policy 21

1. Abbreviations

Information Technology (IT) is a multifaceted domain that demands clarity in terminology for ease of reference and operational coherence. This section elaborates on key abbreviations used throughout the IT Policy of Bareilly International University (BIU). These terms are essential for understanding the technical components, governance frameworks, and standard procedures embedded in the policy.

- **BIU** – Bareilly International University, the governing institution responsible for implementing and overseeing this policy.
- **IT** – Information Technology, referring to the spectrum of computing, software, and networking systems.
- **ICT** – Information and Communication Technology, which emphasizes integrated digital communication services and tools.
- **LAN** – Local Area Network, representing the internal networking system that interconnects devices within the university premises.
- **VPN** – Virtual Private Network, which provides secure access to university resources over public networks.
- **BYOD** – Bring Your Own Device, an operational model allowing personal devices to access institutional networks under approved security conditions.
- **ERP** – Enterprise Resource Planning, a comprehensive software suite for managing academic, financial, and administrative functions.
- **IR** – Institutional Repository, a curated digital archive that stores and disseminates the academic and research output of the university.
- **USB** – Universal Serial Bus, a standard interface for data transfer and device connectivity.

These abbreviations are used consistently throughout the document to maintain clarity, uniformity, and accessibility for all stakeholders engaging with the IT Policy.

2. Introduction

The integration of Information Technology (IT) in higher education has fundamentally transformed pedagogical methods, administrative processes, and research paradigms. At Bareilly International University (BIU), IT is not merely a supporting function but a strategic asset that is essential to achieving academic excellence, operational efficiency, and institutional innovation.

The establishment of this IT Policy arises from BIU's commitment to ensuring optimal utilization of digital resources, enhancing data security, promoting digital literacy, and complying with national and international cyber regulations. It serves as a structured framework for managing digital assets, systems, and users. This policy articulates a proactive approach to resource allocation, data protection, and sustainable technology management.

Given the exponential growth of digital content, virtual classrooms, online examinations, remote collaboration tools, and automated administrative services, the necessity for a comprehensive IT governance document is evident. Additionally, the advent of technologies such as cloud computing, Artificial Intelligence (AI), and the Internet of Things (IoT) makes it imperative to adopt forward-looking, flexible digital strategies.

This policy functions not only as a regulatory document but also as a guide for informed decision-making, responsible user behavior, and strategic investment in IT infrastructure. It underscores BIU's vision of creating a digitally empowered academic environment, fostering innovation, and preparing students and faculty to address global challenges through localized technological advancements.

3. Scope

The scope of the IT Policy at Bareilly International University (BIU) is expansive, comprehensive, and inclusive. It applies to a wide spectrum of users, infrastructure components, and operational domains. All stakeholders including full-time and part-time students, faculty members, administrative staff, research scholars, and authorized external entities—such as contractors, visiting faculty, and project collaborators—fall under the purview of this policy.

This policy governs all physical hardware such as desktops, laptops, servers, printers, routers, switches, and storage devices owned by the university or temporarily connected to the institutional network. Additionally, it includes digital resources such as licensed software applications, databases, digital content repositories, multimedia platforms, and cloud-based tools.

Moreover, the policy encompasses digital services including ERP systems, Learning Management Systems (LMS), the Institutional Repository (IR), examination portals, and communication platforms. It establishes protocols for appropriate conduct in data sharing, content development, and device usage within university premises and beyond, including remote access.

Importantly, this policy applies uniformly across all constituent colleges, departments, campuses, and satellite units operating under the governance of BIU. Whether users access these resources on campus or remotely, they are held accountable for their digital conduct. This wide-ranging scope ensures a uniform implementation of policy principles, harmonized technology use, and seamless digital experiences throughout the institution.

4. Objective

The core objective of the IT Policy of Bareilly International University (BIU) is to provide a strategic and regulatory framework for the development, management, and secure use of Information and Communication Technology (ICT) resources. The policy seeks to support the university's academic, research, administrative, and community engagement missions through secure, ethical, and efficient use of technology.

Key objectives include:

- **Regulating Use of IT Resources**: Define clear responsibilities and expectations for the appropriate use of university IT infrastructure.
- **Data Security**: Safeguard institutional data and personal information from unauthorized access, data breaches, or misuse through stringent access control mechanisms and encryption protocols.

- **Legal Compliance**: Ensure that all software, hardware, and digital platforms adhere to national laws, licensing norms, and international standards for data protection and digital rights.
- **Investment in Technology**: Promote cost-effective and scalable IT investments that align with the university's strategic goals, academic priorities, and operational requirements.
- **Digital Literacy and Capacity Building**: Enhance the digital competence of students, faculty, and staff through ongoing training, user support services, and awareness programs.
- **Sustainability and Green IT**: Encourage environmentally conscious computing practices, such as the use of energy-efficient devices, virtualized systems, and responsible e-waste disposal.
- **Research and Collaboration**: Foster academic innovation and global research visibility through the Institutional Repository and collaborative technology platforms.
- **Governance and Accountability**: Establish a transparent and accountable governance structure for managing IT resources and resolving disputes or violations.

Ultimately, the IT Policy aims to embed technology into the academic fabric of the university, enabling stakeholders to harness its potential for problem-solving, creativity, and academic excellence while preserving institutional integrity and security.

5. Roles and Responsibilities

Effective implementation and enforcement of the IT Policy at Bareilly International University depend on the well-defined roles and responsibilities assigned to various stakeholders. Clarity in duties not only ensures seamless execution of IT services but also reinforces accountability, compliance, and timely resolution of issues. The following roles are crucial to the successful governance of ICT infrastructure:

- **IT Department**: The IT Department is the central authority responsible for the deployment, maintenance, monitoring, and upgradation of all IT assets and services. It is also tasked with setting up network architecture, managing cybersecurity frameworks, ensuring data integrity, enforcing access control protocols, and providing helpdesk support.
- **Faculty Members**: Faculty are expected to use IT resources responsibly, promote digital learning, maintain data confidentiality, and report IT-related issues promptly. They are also encouraged to guide students in ethical use of online resources and digital tools for research and academic work.
- **Students**: Students must adhere to usage guidelines for digital tools, refrain from attempting unauthorized access, avoid sharing login credentials, and ensure that their online activities comply with academic and legal standards. They must seek permission before installing or using software not pre-approved by the university.
- **Administrative Staff**: Staff should use IT systems for their designated official purposes only. They are responsible for maintaining the confidentiality of institutional records and for using enterprise systems like ERP or HRMS in accordance with predefined guidelines.
- **Research Scholars**: Scholars should use the Institutional Repository and licensed software responsibly while ensuring that they comply with ethical research and copyright policies. Any external collaborations involving data exchange must be pre-approved.

- **Vendors/Contractors**: External IT vendors and service providers must abide by university confidentiality agreements and data protection norms. Their access to systems must be monitored, time-bound, and purpose-specific.

6. Acceptable Use

The Acceptable Use Policy at Bareilly International University (BIU) is designed to outline the principles governing the appropriate and ethical use of the university's information technology resources. The goal is to ensure that all users—students, faculty, staff, contractors, and visitors—utilize these resources in a secure, legal, respectful, and academically aligned manner. Acceptable use contributes to a productive learning environment, protects institutional integrity, and ensures the sustainability of digital infrastructure.

Key Principles of Acceptable Use:

- **Academic and Professional Relevance**: IT resources must be used primarily for academic learning, research, administrative work, and university-sanctioned activities. Personal use should be minimal, lawful, and not interfere with university operations.
- **Integrity and Respect**: Users must refrain from engaging in activities that harm, degrade, or negatively affect others. This includes cyberbullying, online harassment, or sending defamatory content via email, social platforms, or communication tools linked to the university.
- **Security Consciousness**: Each user is responsible for maintaining the confidentiality of their credentials and must report suspicious activity immediately. Installing unapproved applications or bypassing university security measures is strictly prohibited.
- **Legal and Ethical Boundaries**: It is forbidden to access, create, download, or share pirated software, copyrighted media, or offensive material including hate speech, pornography, and violent propaganda.
- **Network Discipline**: Bandwidth is a shared resource and must be used judiciously. Streaming, large file transfers, and cloud backups should be scheduled during off-peak hours with prior IT department notification.
- **Non-Commercial Use**: University resources must not be used for personal financial gain, product advertisement, online trading, or unauthorized fund collection. Such acts are considered a severe breach of policy.
- **Email Etiquette**: Institutional email must be used responsibly. Sending mass emails without authorization, phishing messages, or chain letters violates ethical and legal guidelines.

Enforcement and Compliance: Violations of the Acceptable Use Policy may result in disciplinary action, which can include temporary or permanent revocation of IT privileges, academic penalties, or legal action depending on the severity of the offense. The IT Department, in consultation with university authorities, holds the authority to investigate misuse and enforce corrective measures.

7. IT Hardware Installation Policy

The IT Hardware Installation Policy at Bareilly International University (BIU) ensures that all computer hardware and peripheral devices deployed across the university's campuses meet quality, security, and compatibility standards. The objective of this policy is to streamline the process of hardware procurement, installation, and maintenance while maintaining an inventory that aligns with the institution's academic and administrative goals.

Procurement and Approval:

- All IT hardware must be procured through a centralized system managed by the university's IT Department.
- Hardware requests must be justified through need-based proposals submitted by department heads.
- Approval must be obtained from the Finance and IT Committees before any procurement is initiated.

Installation Standards:

- Only IT Department personnel or authorized service providers are permitted to install or configure hardware on university premises.
- Devices must be installed in accordance with ergonomic and safety standards.
- All installed hardware must be registered in the university's digital asset inventory and labeled with an official asset tag.

Compatibility and Integration:

- New hardware must be compatible with the existing network infrastructure, software ecosystem, and power supply.
- Peripheral devices such as printers, projectors, and biometric systems must be integrated under supervision to ensure seamless performance.

Security Considerations:

- Any hardware device that connects to the university network must comply with security policies, including endpoint protection, firmware validation, and port access control.
- Unauthorized modification, tampering, or relocation of installed hardware without IT Department consent is strictly prohibited.

Maintenance and Support:

- Routine preventive maintenance schedules will be maintained for critical infrastructure, including servers and routers.
- Users must report malfunctioning or damaged equipment to the IT helpdesk for inspection and service.
- A record of maintenance logs and equipment life cycles must be maintained by the IT Department.

Disposal and Replacement:

- Hardware deemed obsolete or irreparable must be retired following the university's e-waste disposal guidelines.
- Replacement requests must be supported with performance reports and approval from designated committees.

Audit and Compliance:

- Periodic audits will be conducted to verify the location, condition, and usage of IT hardware.
- Non-compliance with hardware policies may result in disciplinary actions, including revocation of hardware privileges.

8. Software Installation and Licensing Policy

The Software Installation and Licensing Policy at Bareilly International University (BIU) is intended to manage, regulate, and ensure the ethical and lawful use of all software within the university environment. The policy is crucial in protecting the university from legal risks, ensuring compatibility with IT systems, and maintaining the integrity of academic and administrative operations.

Procurement and Licensing:

- All software must be purchased or sourced through the IT Department to ensure validity and compliance with licensing agreements.
- Only licensed, open-source, or institutionally-approved software is allowed for installation on university-owned devices.
- Site licenses or volume licenses will be preferred where multiple installations are required to optimize cost and manageability.
- Detailed records of all software licenses, including renewal dates and usage statistics, must be maintained and audited annually.

Installation Process:

- Only authorized personnel from the IT Department may install software on university systems.
- Requests for new software must be submitted in writing, reviewed for technical feasibility, and approved by relevant authorities before installation.
- Standard operating environments will be maintained for academic labs, administrative departments, and specialized research setups to ensure uniformity.

Security and Compatibility:

- Prior to installation, all software must be scanned for malware and tested for compatibility with the university's hardware and network environment.
- Software known to interfere with institutional systems or which poses a security threat will be blacklisted.

User Responsibilities:

- Users are strictly prohibited from installing unauthorized software or bypassing installation protocols.
- Software licensed to the university must not be copied, shared externally, or used for personal or commercial purposes.
- Users must report expired licenses or malfunctioning software to the IT Department immediately.

Freeware and Open-Source Tools:

- The use of open-source software is encouraged, provided it is reviewed for compliance with institutional standards and does not introduce vulnerabilities.
- Any freeware or open-source tool used must be documented, reviewed, and approved by the IT Department before deployment.

Compliance and Auditing:

- Periodic software audits will be carried out to verify licensing compliance, usage efficiency, and system compatibility.
- Users found violating this policy will be subject to disciplinary action and revocation of IT privileges.

9. Use of IT Devices on BIU Network

The Use of IT Devices on Network Policy at Bareilly International University (BIU) ensures that all personal and institutional devices accessing the university's network are compliant with security, compatibility, and usage standards. This policy addresses the protocols and expectations for connecting desktops, laptops, tablets, mobile phones, and other smart devices to the university's wired and wireless networks.

Device Registration and Authorization:

- All devices must be registered with the IT Department prior to connecting to the university's intranet or internet networks.
- Devices must be tagged with a unique user ID and MAC address to allow monitoring and access control.
- Unauthorized devices will be automatically blocked by the university's firewall and flagged for IT review.

Security Compliance:

- Devices must have updated antivirus software, secure firewall settings, and the latest security patches.
- Users must implement strong passwords and enable automatic screen-lock functions.
- Lost or stolen devices must be reported immediately so that network access can be revoked.

Use of Personal Devices (BYOD):

- Personal devices may connect to the university Wi-Fi only after approval and configuration by the IT Department.
- Users must agree to limited IT oversight, including periodic security scans and usage audits.
- Storage of sensitive or official university data on personal devices is discouraged and must be encrypted when necessary.

Acceptable Device Usage:

- Devices may be used for official university business, research, and approved academic purposes only.
- Streaming services, torrent downloads, and excessive gaming on the university network are prohibited.
- Any attempt to bypass content filters or firewalls will be treated as a serious violation.

Monitoring and Enforcement:

- All device activity on the BIU network is subject to logging and monitoring in accordance with the university's privacy and surveillance policy.
- Suspicious activities may trigger automatic disconnection, reporting to university authorities, and temporary or permanent ban from the network.

IT Support for Network Access:

- The IT Department will provide manuals, FAQs, and hands-on support for users who face difficulties connecting to the network.
- Troubleshooting will include diagnosis of configuration errors, virus removal, and reauthorization of compliant devices.

Network Access During Exams:

- During online assessments or digital evaluations, only university-provided devices may be allowed unless explicitly approved.
- Device logs may be reviewed post-exam to verify compliance with academic integrity protocols.

10. Desktop Devices

The use of desktop devices within Bareilly International University (BIU) is governed by a policy that emphasizes operational consistency, security compliance, and resource optimization. This policy outlines the standards and expectations related to the use, maintenance, and management of desktop computers across university departments, laboratories, libraries, and administrative offices.

Allocation and Setup:

- Desktop systems will be allocated based on academic and administrative needs following departmental requisitions approved by the university administration.

- Initial setup, configuration, and installation of operating systems and essential software will be managed solely by the IT Department.
- All devices will be assigned a unique asset identification number and entered into the university's digital inventory management system.

Authorized Use:

- Desktop devices are to be used exclusively for university-related activities, including teaching, research, data processing, communication, and student support services.
- Access to administrative systems such as ERP, examination portals, and financial software must be role-based and approved by department heads.

Security Measures:

- All desktop devices must have antivirus software, firewalls, and security patches regularly updated by the IT Department.
- Users must not disable or alter any security configurations or monitoring tools installed by IT personnel.
- Access must be protected by strong, periodically updated passwords, and devices must be locked when unattended.

Maintenance and Repairs:

- Users must report technical issues immediately to the IT Helpdesk.
- Repairs and upgrades shall only be carried out by authorized university IT staff or approved vendors.
- Periodic maintenance checks will be conducted to ensure devices function efficiently and securely.

Software Usage:

- Only software approved and installed by the IT Department is allowed on desktop systems.
- Unauthorized installation of games, pirated software, or resource-heavy applications is strictly forbidden.

Data Storage and Backup:

- Users are encouraged to store work-related files on university cloud storage platforms or network drives to ensure data backup and recovery.
- Personal data must not be stored on desktop devices connected to the institutional network.

Energy Efficiency and Shutdown Protocols:

- Users must shut down or log off from desktops at the end of each workday to conserve energy and enhance system longevity.
- Systems will be configured to enter automatic sleep mode during periods of inactivity.

Disposal and Replacement:

- Old or damaged desktop systems will be decommissioned according to university e-waste and asset disposal policies.
- Replacement requests must include justification and will be evaluated during annual IT resource reviews.

11. Sharing of Data

Data sharing is a critical component of modern academic and administrative environments. At Bareilly International University (BIU), this policy outlines how data—ranging from academic research to operational records—should be shared responsibly, securely, and ethically. The policy ensures that shared data maintains its confidentiality, integrity, and utility while aligning with university regulations and applicable legal standards.

Scope of Shared Data:

- Institutional data includes student records, staff files, research data, financial transactions, academic assessments, and administrative reports.
- Shared data may be internal (between departments, faculties, and administrative units) or external (with government agencies, accreditation bodies, research collaborators, or third-party vendors) based on necessity and approval.

Authorization and Approval:

- All data-sharing activities must be pre-approved by the concerned Head of Department (HoD) and/or administrative authority.
- Sensitive data, such as personal identification numbers, medical records, and financial details, requires additional clearance from the Registrar or Data Protection Officer.

Methods of Sharing:

- Data must be shared using secure, encrypted platforms approved by the IT Department (e.g., official email, secure portals, encrypted cloud services).
- Use of public storage platforms (such as free online drives or third-party apps) for university data is strictly prohibited.

Data Classification and Labeling:

- All data intended for sharing must be classified (e.g., Confidential, Internal Use, Public) and labeled accordingly.
- Confidential or restricted data must carry a disclaimer about its appropriate use and intended audience.

Responsibilities of Data Handlers:

- Employees and students must not share data beyond its intended recipients or for unauthorized purposes.
- All shared data must be accurate, complete, and up to date to ensure it serves its intended function without causing harm.

Data Retention and Retrieval:

- Shared data must be retained in a secure repository for a minimum period as prescribed by the university's records retention policy.
- Data retrieval logs will be maintained for audit and accountability.

Third-Party Access and Agreements:

- When data is shared with third parties, a Memorandum of Understanding (MoU) or Non-Disclosure Agreement (NDA) must be signed outlining the purpose, scope, duration, and confidentiality clauses.
- Third parties must not reuse, resell, or modify the data for purposes outside the agreement.

Violation and Penalty:

- Unauthorized data sharing is a serious breach and may result in suspension of IT privileges, academic penalties, employment actions, or legal proceedings.

12. Use of Portable Devices

The Use of Portable Devices Policy at Bareilly International University (BIU) aims to regulate the access, security, and permissible use of mobile and portable digital devices within the university ecosystem. With the growing reliance on mobile computing, this policy ensures the protection of university data while supporting flexibility and remote access.

Definition of Portable Devices:

- Portable devices include but are not limited to laptops, tablets, smartphones, USB drives, external hard disks, and any wearable or handheld digital equipment.

Usage Permissions and Scope:

- Students, faculty, researchers, and staff may use approved portable devices for academic and administrative purposes.
- The devices may connect to university Wi-Fi and intranet services upon registration and security clearance by the IT Department.

Device Registration and Approval:

- All devices must be registered with the IT Department, and users must provide device details (model, OS, MAC address, serial number).
- Personal devices accessing sensitive university data must be enrolled in the Mobile Device Management (MDM) system if applicable.

Security Requirements:

- Devices must have up-to-date antivirus protection, encrypted storage, and secure access protocols (passwords, PINs, biometric authentication).