ज्ञान शांति मैत्री

महात्मा गांधी अंतरराष्ट्रीय हिंदी विश्वविद्यालय

Mahatma Gandhi Antarrashtriya Hindi Vishwavidyalaya

(संसद द्वारा पारित अधिनियम 1997, क्रमांक 3 के अंतर्गत स्थापित केंद्रीय विश्वविद्यालय)

(A Central University established by Parliament by Act No. 3 of 1997)

क़ादर नवाज़ ख़ान
कुलसचिव (कार्यवाहक)
Kadar Nawaz Khan
Registrar (Acting)

दूरभाष/Phone : + 91 - 7152 - 230902
ई–मेल/E-mail : registrar@mgahv.in

क्रमांक : 003/1998/का.प./10(88)-17/2025/320

दिनांक : 02.03.2026

परिपत्र

कार्य-परिषद् द्वारा दिनांक 07.01.2026 को सम्पन्न 88 वीं बैठक में मद संख्या- 15 के अंतर्गत लिए गए निर्णय के आलोक में विश्वविद्यालय की तकनीकी अधिसंरचना को सुदृढ़ करने हेतु संलग्न अद्यतन आईटी पॉलिसी लागू की जाती है।

क़ादर नवाज़
(क़ादर नवाज़ ख़ान)
04/03/26

प्रतिलिपि (ई-मेल द्वारा):

1. कुलपति सचिवालय
2. समस्त अधिष्ठाता, विभाग अध्यक्ष/प्रमुख एवं केंद्र निदेशक
3. निदेशक, वर्धा समाज कार्य संस्थान
4. निदेशक, आंतरिक गुणवत्ता सुनिश्चायन प्रकोष्ठ
5. अकादमिक निदेशक, क्षेत्रीय केंद्र प्रयागराज
6. प्रभारी, क्षेत्रीय केंद्र, कोलकाता
7. प्रभारी, सर्वज्ञ श्री चक्रधर स्वामी मराठी भाषा तथा तत्त्वज्ञान अध्ययन केंद्र, रिद्धपुर (अमरावती)
8. पुस्तकालयाध्यक्ष
9. कुलसचिव कार्यालय
10. वित्ताधिकारी (कार्यवाहक)
11. परीक्षा नियंत्रक
12. अकादमिक विभाग
13. अन्य प्रशासनिक विभाग/कार्यालय/प्रकोष्ठ
14. प्रभारी-'लीला', विश्वविद्यालय की वेबसाइट पर अपलोड करने हेतु
15. रक्षित पत्रावली।

Mahatma Gandhi Antarrashtriya Hindi Vishwavidyalaya, Wardha

IT Policy

1. Introduction

Mahatma Gandhi Antarrashtriya Hindi Vishwavidyalaya, Wardha is proposing to have its own IT Policy that works as guidelines for using the university's IT Infrastructure including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (IT)". The purpose of this Information Technology (IT) Policy is to provide a framework for the effective and secure use of the IT resources at Mahatma Gandhi Antarrashtriya Hindi Vishwavidyalaya, Wardha. It establishes guidelines for access, usage, data security and infrastructure management to support the university's academic, administrative and research objectives. In the light of National Education Policy (NEP) and following recent epidemic situations, the policy document addresses e-education needs and ensures preparedness for implementation of hybrid mode of learning.

IT policies and related standards apply to all users across the entire Mahatma Gandhi Antarrashtriya Hindi VishwaVidyalaya, Wardha and all centers of university including campus visitors. This policy applies whether the university's information resources are accessed on- or off-campus.

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

2. Objectives:

a) Optimal use of IT resources.
b) Safeguard the confidentiality, integrity and availability of university data.
c) Responsible use of IT infrastructure.
d) Comply with national laws (e.g., IT Act 2000, UGC and MeitY guidelines).
e) Support innovation in teaching, learning, and research.

3. Purpose and Scope of IT Policy:

MGAHV Provides IT resources to its end-user to enhance their efficiency and productivity. These resources are meant as tools to access and process information

related to their areas of work. For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated there with.

All IT systems including hardware, software, network infrastructure and data.

These Resources are-

1. Network Devices- wired/ wireless
2. Internet Access devices
3. Official Websites, web applications
4. Official Email services
5. Data Storage
6. Desktop / Laptop server computing facility
7. Software
8. Documentation facility (Printers/Scanners)
9. Multimedia Contents and equipment
10. ICT resources

3.1 Scope-

This policy applies to all University students, faculty and staff, and all others using computer and communication technologies, including the University's network, whether personally or University owned, which access, transmit or store University or student information.

This policy also applies to all other individuals and entities granted use of University Information, along with contractors, temporary employees, and others as identified by university.

This policy applies to:

a) All students, faculty, staff, research scholars, and contractors
b) Students (Diploma, UG, PG, Research etc.)
c) All Employees (Permanent/ Temporary/ Contractual)
d) Guests and Visitors

---

4. IT Governance:

a) The **IT Cell** with University Administration will oversee the implementation and enforcement of the policy.
b) The **IT Cell** will periodically review and update the policy.

5. **Acceptable Use:**
   a) Users must use university IT resources **only for academic, administrative, professional and research purposes**.
   b) Activities such as hacking, use of pirated software, unauthorized data access, and cyber bullying are strictly prohibited.
   c) Internet and email usage must comply with Indian laws and university rules.

6. **User Accounts and Access Control:**
   a) Unique IDs and passwords will be issued to authorized users.
   b) Users are responsible for maintaining the confidentiality of their credentials.
   c) Access to sensitive systems (ERP, LMS, finance etc.) will be role-based and audited periodically (if applicable).

7. **Access to the MGAHV Wired/Wireless network:**

For connecting to a MGAHV Wired/Wireless network, user should ensure the following:

7.1 A user should register the access device and obtain one time approval / permission from concern authorities then only LILA (Laboratory In Informatics for Liberal Art) will provide the access to the MGAHV **Wired/Wireless** network.

7.2 Other Wireless client systems and wireless devices should not be allowed to connect to the MGAHV wireless access points without due authentication and approval of permission from concern authorities.

7.3 LILA may block content over the Internet/Intranet which is in contravention of the relevant provisions of the Government Laws and other applicable laws or which may pose a security threat to the **Wired/Wireless** network and as per the order of competent authorities of MGAHV.

7.4 LILA may also block content, which, in the opinion of competent authorities of the University, is inappropriate or may adversely affect the network security and productivity of the users/organization.

8. **Network/Server and Internet Policy:**
   a) The university will maintain secure wired and wireless networks across campus.

b) Use of personal routers, hotspots, or network switches without prior approval is prohibited.

c) Network traffic may be monitored to prevent misuse and ensure performance.

8.1 Individual/Stakeholders Responsibilities for University Wired/Wireless Network usage-

Individuals must not:

8.1.1 Use the internet or email for the purposes of harassment or abuse.

8.1.2 Use profanity, obscenities, or derogatory remarks in communications.

8.1.3 Access, download, send or receive any data (including images, audio, video etc.), which competent authorities of the University considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.

8.1.4 Use the internet or email to gambling.

8.1.5 Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam emails.

8.1.6 Place any information on the Internet that relates to University, alter any information about it, or express any opinion about University, unless they are specifically authorized to do this.

8.1.7 Send unprotected sensitive or confidential information externally.

8.1.8 Make official commitments through the internet or email on behalf of university unless authorized to do so.

8.1.9 In any way infringe any copyright, database rights, trademarks or other intellectual properties.

8.1.10 Leave confidential material on printers or photocopiers pool.

8.1.11 Violate the IT ACT of GOI provided from time to time.

8.2 Guidelines for Desktop/PC/Laptop etc Users-

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

The following recommendations include:

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

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

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

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

8.2.5 Don't open email or attachments from unknown sources.

8.2.6 The guest account should be disabled in confidential sections.

8.2.7 Disconnect from the Internet when not in use.

8.2.8 When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original source.

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

8.2.10 Do not allow anyone else to use their user ID and password on MGAHV IT system

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

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

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

8.2.14 All shared folders should be password protected.

8.2.15 Remote Login should be disabled and only in special cases it would be permitted with permission of LILA /IT CELL.

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

---

9. Data Management and Security:

a) All institutional data (employee's data, student records, research data, financial etc.) must be stored in authorized servers or cloud platforms (if needed).

b) Users must not store sensitive data on personal devices unless encrypted and authorized.

c) IT Cell will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user.

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

---

10. Backups of Data:

a) Individual users are responsible to perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible and the loss of data is the sole responsibility of the individual.

b) Regular data backups must be maintained by concerned office/department/cell of university.

---

11. Wi-Fi implementation and usage:

11.1. Wi-Fi Access and locations-

11.1.1 Wi-Fi Access Point: Wi-Fi facilities may be made available at canteen, library, hostels, department/cell/section, laboratories, guest house and residences within Campus etc. The decision of LILA/ IT CELL will be final to decide the location of such access points.

11.1.2 Wi-Fi Access Points may be placed temporarily on demand in auditorium and other places, for conference, workshops, symposia and any other important events.

11.1.3 In special cases the individual or department may approach the LILA/ IT CELL to get proper secure configuration and registration of the personal/ department's Access Points or routers with proper approval of the concerned head.

11.2 Wi-Fi Usage -

11.2.1 The individual user will be responsible for his/her Wi-Fi usage.

11.2.2 Solicited and ethical usage is expected from the users.

11.2.3 The Internet Access through Wi-Fi is filtered access. Possible phishing, spurious, unsolicited or obscene sites, gaming sites, some shopping/multimedia streaming sites may be blocked at firewall level.

11.2.4 There shall be a per day/month usage quota for internet users. Quota may depend on nature of work or as defined by concerned department.

11.2.5 The users will access the University Resources properly and will not try to harm the resources.

11.2.6 For respected guests/invitees staying in the campus Wi-Fi access is given on demand by the corresponding hosts. It is password-based access. Passwords must be changed periodically by concerned person.

11.3 Misuse and actions -

11.3.1 If a user or his/her device is causing any harm to university resources or other users, then such a user will be initially advised by the concerned department or LILA to stop such activity. After knowing User's intention that device will be verified by technical team and the corresponding Head of the department will be informed accordingly. If found guilty, appropriate action will be taken by competent authorities of the University.

11.3.2 A virus/malware infected device may create noticeable network traffic or attempt cyber-attacks. Then the user will be notified and his/her access shall be blocked until the infected device is cleaned/ free from viral infection.

---

12. Internet Access:

a) The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. Network IDs will only be established for students, staff and faculty who are currently affiliated with the University. Students, staff and faculty who leave the University will have their Net Access ID and associated files deleted within 15 days.

b) No user will be allowed more than one Net Access ID at a time, with the exception that faculty or officers, who hold more than one portfolio, are entitled

to have internet Access ID related to the functions of that portfolio. Multiple Logins (if permitted) may be provided on a Net Access ID.

c) In special cases like workshop/seminar/conferences/meetings etc. access could be permitted to the concerned department.

12.1 Limitations on the use of Resources/Data-

a) On behalf of the University, LABORATORY IN INFORMATICS FOR LIBERAL ART (LILA) reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts (as defined by the university from time to time) of storage space or whose actions otherwise limit the use of computing resources for other users.

b) The data related to gaming, harmful software and other such activities which harms the university network is not allowed.

12.2 Ethics and Etiquette-

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

---

13. IT Hardware Installation:

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

13.1 Primary User

a) Computer System issued individual(Administrative officers/Faculty/staff/research scholar) that individual will be responsible for that system.

b) Those systems in the lab/office, department Head should make an arrangement and make a person (lab coordinator) responsible for compliance.

13.2 End User Computer Systems

Computer systems, if any, related to "end users" that are acting as servers which provide services to other users on the Intranet/Internet are considered under this policy as "end-users" computers.

13.3 Warranty and Annual Maintenance Contract -

13.3.1 Any IT equipment purchased by the University and provided to primary users may be maintained under annual maintenance contract.

13.3.2 Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract.

13.3.3 The above said maintenance will be under the supervision of the IT Cell.

13.4 Power Connection to Computers and Peripherals -

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

13.4.2 All the power connection related issues/ installation of ups/earthing/wiring related issues will be dealt with by the Engineering Section/Campus Development of MGAHV.

13.5 Shifting Computer from One Location to another –

Computer systems may be moved from one location to another with prior written intimation to the LILA, although the inventory and stock/assets register and the record of computer identification names and serial numbers are maintained by store and purchase department. As and when any deviation is found for any computer system, network connection would be disabled and the same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs the LILA in writing/by email, connection will be restored.

13.6 Non compliance -

MGAHV faculty, staff, Guest users and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computers resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even the whole university. Hence it is critical to bring

all computers into compliance as soon as they are recognized not to be non-compliant.

14.0 Software Licensing and Use:

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

14.0.2 Respecting the anti-piracy laws, University IT policy does not allow any unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, the university will hold the department/individual personally responsible for any unauthorized software installed on the computers located in their department/individual's rooms.

14.1 Operating System and its Updating -

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

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

14.2 Antivirus Software and its updating -

14.2.1 Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system safe from Virus, Malware, and Trojan etc.

14.2.2 User should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use.

14.2.3 If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from LILA or any service-providing agency.

14.2.4 Do not remove or disable anti-virus software.

14.2.5 Do not use unauthorized/ not licensing Antivirus Solution.
14.2.6 Centralized Firewall/UTM or network base antivirus shall be installed.

---

15. Backups of Data:

a) Individual users are responsible to perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible and the loss of data is the sole responsibility of the individual.

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

---

16. Cyber security:

16.1 Antivirus and firewall systems will be maintained and regularly updated.
16.2 Users must immediately report any cyber security incidents to cyber crime reporting portal, Government of India i.e. cybercrime.gov.in and cyber crime helpline number 1930 or as updated by GoI from time to time as well as to LILA.
16.3 Mandatory awareness programs will be conducted regularly by LILA.

---

17. Support and Maintenance:

a) LILA is there for technical support.
b) Preventive and corrective maintenance of computer systems and ICT use will be scheduled for all university employees and students by conducting seminars, training programs by LILA on regular intervals.

---

18. Use of Personal Devices (BYOD):

a) Personal devices must adhere to security standards if used for university work.
b) University is not responsible for loss or damage to personal devices.

---

19. Policy Violations:

Violations may result in disciplinary action, including suspension of access, legal action, or expulsion/termination if university found it suitable.

20 - Network Device Connectivity and Installation:

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

20.1 IP Address Allocation-

20.1.1 Any computer (PC/laptop/Server) that will be connected to the university network should have an IP address assigned by the LILA through DHCP server.

20.1.2 Any IP base device like network printer, smart TV, biometric machine, CCTV DVR, IP Camera, Video conferencing device, IP Phone etc. is to be installed at any location (with prior approval of university), then the concern user should contact LILA and get proper IP Address.

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

20.1.4 Following a systematic approach, the range of IP addresses that will be allocated to each department/section/hostel etc. is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool.

20.2 Wireless Local Area Networks-

20.2.1 This policy applies, in its entirety of campus (to School, department, administrative section, hostels, or division etc.) wireless local area networks. In addition to the requirements of this policy, schools, departments, or divisions must register each wireless access point with LILA including Point of Contact information. LILA Will be responsible for creating wireless access points.

20.2.2 School, departments, or divisions must operate wireless local area networks with restricted access via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

20.2.3 If individual departments/schools etc. wants to have an inter-building wireless network, prior to installation of such network, it should obtain permission from the University authorities.

20.3 Structured Cabling as a part of New Buildings-

20.3.1 All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan.

20.3.2 Engineering Cell/Section may make provisions in their designs for network points/access points in each room and in the corridors based on the input provided by LILA. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

---

21 Video Surveillance/CCTV Monitoring:

21.1 The system

21.1.1 The system comprises:

Fixed position cameras; Pan Tilt and Zoom cameras; Monitors/Television/LED/LCD panels: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs; DVR/ NVR; Network Switches etc.

21.1.2 Cameras will be located at strategic points (as decided by competent authorities) on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

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

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

21.2 . Purpose of the system

The system has been installed by the university with the primary purpose of reducing the threat of crime generally, protecting university's premises and helping to ensure the safety of all staff, students and visitors with respect for the individuals' privacy. These purposes will be achieved by monitoring these units-

21.3 The Security Control Room

21.3.1 Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day

throughout the whole year. Monitors should not be visible from outside the control room.

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

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

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

21.4 Staff: Security Control Room

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

21.5 Recording

21.5.1 Digital recordings are made using digital video recorders Network Video Recorders operating in time lapse mode. Incidents may be recorded in real time.

21.5.2 Images and Recordings will normally be retained for **fifteen** days from the date of recording, and then automatically overwritten and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

21.5.3 All hard drives and recorders shall remain the property of the university until disposal and destruction.

---

22. Email and Communication:

a) Official communication must be done via university-assigned email accounts.
b) Email should not be used for spamming, personal business, or chain letters.

22.1 Email Account Management –

22.1.1 Based on the request of the respective department/Centre, LILA will create ID. Some Designation based ids are recommended for officers dealing with the public. University staff/ teachers/students who quit, resign, superannuate or completes the course shall be allowed to retain the name-based e-mail address i.e. userid@hindivishwa.ac.in for 2 months post resignation or superannuation or completes the course. The personal details of His/her email account shall be updated and his/her account shall be delisted from all the concerned group emails immediately upon leaving the University.

22.1.2 Provision of university domain email ID for student-

It is not possible to give email ID to all students of university because it leads financial burden on university. All students of Master degree and research program student should be given university email ID for their research based academic use. And this email will be valid up to their course period (as decided by the university on the basis of academic ordinance) only.

22.2 Delegated Admin Console –

For security reasons, no other department/center/section/unit may be allowed to access the Administrator Account. Only LILA is authorized to create/ delete/ change the password of user ids under that respective domain as and when required.

22.3 E-mail Domain –

By default, the address "userid@hindivishwa.ac.in" shall be assigned to the users. The user id shall be created as per the addressing policy mentioned in email creation form.

22.4 Use of Secure Passwords-

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

22.5 Privacy –

Users should ensure that emails are kept confidential. Users must ensure that information regarding their password or any other personal information is not shared with anyone.

22.6Responsibilities of Users/Appropriate Use of E-mail Service –

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

22.6.1 For personal communication, reasonable use of the email service is permitted provided it is not:

a. Of commercial/profit-making nature or used for personal financial gains.
b. In conflict with University rules, regulations, policies, and procedures including the email policy.
c. In conflict with the end-user obligations towards the University as employer.

22.7 Security Incident Management Process-

A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of university data. Security incidents can be due to factors like malware, phishing, loss of a device, compromise of an e-mail id etc. It shall be within the right of the LILA to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service. Any security incident, noticed or identified by a user, must immediately be brought to the notice of the LILA.

22.8 Deactivation-

In case of threat to the security of the University service, the e-mail id and other IDs and services (Samarth, internet Access ID, email ID etc.) being used to impact the service may be suspended or deactivated immediately by the LILA. Subsequent to deactivation, the concerned user and the competent authority of that respective Department/Cell/Section shall be informed.

---

23. Review and Amendment:

a) This policy will be reviewed every 2 years or as required by changes in law or technology.

b) Amendments must be approved by the competent authorities of University.

---

24. General Information Technology Usage Guideline:

24.1 Prohibited Use-

Users must not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation

of applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.

24.2 Copyrights and Licenses-

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

24.3 Social Media-

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

24.4 Political Use-

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

24.5 Personal Use-

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

24.6 Commercial Use-

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

24.7 Open Source Asset-

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

24.8 Password Policy-

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

24.9 Safeguard your Equipment-

Adopt Security measures that protect your equipment against theft, fire and explosives.

24.10 Protect your Power Supply-

Protect your equipment from power failures and electrical anomalies. Make sure that your power supplies will be provided without interruption and comply with the specifications provided by equipment manufacturers. Also consider multiple power feeds.

24.11 Secure your Cables-

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

24.12 Maintain your Equipment-

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

25. Purchase/ Procurement Policy:

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

25.1 Procedure-

a) The purchase of computer hardware, software, networking equipment and allied material shall be done after the approval from the Central/Local Purchase committee.

b) At least one member nominated by competent authority from LILA will be part of CPC/LPC for this purpose.

c) LILA will check the minimum configuration and warranty of the above said and may suggest accordingly.

d) The purchase procedure shall be as per the university rule.

25.2 Warranty-

Procurement of IT Assets should cater for onsite warranty, as far as practicable for extended period. The warranty should cover all items of non-consumable nature including batteries of UPS, laptops and such other portable IT devices. The scope of warranty of Software should also include patches,

updates/upgrades and associated changes of application and provision of help desk facility for providing support in structured and time bound manner.

26. Condemnation and Disposal of IT equipment:

The IT policy will adhere to the condemnation and disposal policy already formulated by the university.

27. Role and Responsibilities:

27.1 Responsibilities of LILA-

27.1.1 Campus Network Backbone Operations-

The campus network backbone and its active components are administered, maintained and controlled by LILA.

27.1.2 Physical Demarcation of Campus Buildings' Network –

Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of LILA.

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

a) **Network Expansion:** Major network expansion is also the responsibility of LILA. Every 3 to 5 years, LILA reviews the existing networking facilities, and needs for possible expansion. Network expansion will be carried out by LILA when the university makes the necessary funds available.

b) **Wireless Local Area Networks:**

Where access through Fiber Optic/UTP cables is not feasible, in such locations LILA considers providing network connection through wireless connectivity.

27.1.3Providing Net Access IDs and email Accounts-

LILA provides Net Access IDs and email accounts as mentioned in the point 12 of this policy.

27.1.4 Network Operation-

LILA is responsible for the operation of a centralized Network Operation. The campus network and Internet facilities are available 24/7 a week. All network

196

failures and excess utilization are reported to the LILA technical staff for problem resolution.

27.1.5 Network Policy and Technology Standards Implementation-

LILA may take reasonable steps necessary to compliance with network related policies that are designed to protect security of the campus network backbone.

27.1.6 Receiving Complaints -

LILA may receive complaints from the users if any of the users is not able to access the network due to a network related problem at the user end. Such complaints may be generally through SAMARTH PORTAL to LILA. The designated person in LILA receives complaints from the users and coordinates with the user/service engineers or with the internal technical team to resolve the problem within a reasonable time limit. LILA will be responsible only for solving the network related problems or services related to the network. LILA may also receive suggestions for the smooth and timely delivery of services.

27.1.7 Disconnect Authorization-

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

27.1.8 Enforcement-

LILA periodically scans the University network for provisions set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines. Such disconnection shall be informed to the concerned individual and shall also be informed on conditions for reconnection (with due permission of competent authority of university).

The LILA (In charge) will be responsible for allocation of roles to the personnel under LILA for better functioning of IT related issues.

Backing up Critical data and application residing on Servers while ensuring safe custody and accounting of media used for it.

27.2 Responsibilities of Department or Sections-

27.2.1 Any Centre, department, or Section or other entity can connect to the University network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the university. The user account will be provided by LILA, upon filling up the prescribed application form and submitting it to LILA.

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

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

27.3 Responsibilities of the Administration-

LILA needs latest information from the different Administrative Units of the University for providing network and other IT facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the MGAHV web site up-to-date in respect of its contents.

27.3.1 The information that is required could be broadly of the following nature:

a) Information about New Appointments/Promotions.
b) Information about Superannuation/Termination of Services, or about someone who is no more a part of university due to any other reason.
c) Information of New Enrolments.
d) All notices, circulars to show on notice section of MGAHV website should be sent by proper channel in time.
e) Information on Expiry of Studentship/Removal of Names from the Rolls.
f) Any action by the university authorities that makes individuals ineligible for using the university's network facilities.

28. Policy Monitoring:

28.1 Policy Dissemination-

28.1.1 The IT Committee of the MGAHV should ensure proper dissemination of this policy.

194

28.1.2 The IT Committee may use newsletters, banners, bulletin boards etc. to facilitate increased awareness about this policy amongst their users.

28.1.3 Orientation programs for new recruits shall include a session on this Policy.

28.1.4 For implementation of this policy, the IT committee shall be competent to suggest modifications in rules and the University will amend necessary rules as suggested by IT committee or otherwise from time to time.

28.2 Violation of Policy-

Any violation of the basic objectives and areas mentioned under the IT Policy of the University shall be considered as a violation and as a misconduct and gross misconduct under University Rules.

28.3 Access Control Policy-

Without permission mobile phones or any gadgets or electronic photography devices are not allowed in restricted or prohibited areas or in confidential documents rooms. Users are encouraged to be vigilant and to report any suspected violation of this policy immediately to the concerned office.

28.4 Review and Monitoring of Policy-

The Policy document needs to be reviewed at least once in two years and updated if required, so as to meet the pace of the advancements in the IT related development in the industry.

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

28.5 Change Management-

IT Policy necessarily evolves with changes in IT infrastructure and threat scenario. Once promulgated, further changes in IT policy would be reflected as additions/deletions to this document. Anything that is not covered in this policy will be decided by the Vice Chancellor. The Vice Chancellor has

authority to interpret this policy and any decision taken by the Vice Chancellor will be final and binding on everyone.

29. IT Cell-

IT cell includes personnel of LILA and at least one person (preferably from IT background) from each Section, department, or division may be assigned as a member.

30. The IT Committee-

The IT Committee shall be an apex advisory and recommending body on all matters pertaining to IT in the University and shall report to competent authority.

The IT Committee shall consist of -

1. Registrar as Chairperson,
2. Two faculty members (nominated by VC for the period of 2 years)
3. System Analyst – (Member),
4. CISO(Chief Information Security Officer)-(Member),
5. Software Associate-(Member),
6. Legal advisor from LAW department-(Member),
7. Technical assistant-(Member Secretary)

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

For implementation of this policy, the IT committee shall be competent to suggest modifications in rules and the University will amend necessary rules as suggested by IT committee or otherwise from time to time.

31. Meetings:

Meetings of the IT Committee shall be convened at least twice in a year by the Chairperson.

32. Removal of Difficulties:

Notwithstanding anything contained in this policy, the Vice Chancellor may take measures, as may be necessary, in accordance with provisions of national laws (e.g., IT Act 2000, UGC and MeitY guidelines etc).

Annexures-

1. **Internet Use Form for Teacher/Officer/employee of University**
2. **Internet Use Form for Students of University**
3. **Internet Use Form for Guest Faculty/Guest of University**
4. **Email Id Application Form for Teacher/Officer/employee of University**
5. **Email Id Application Form for Students of University**

1. Internet Use Form for Teacher/Officer/employee of University

इंटरनेट उपयोग करने हेतु आवेदन-पत्र

शिक्षक/अधिकारी/कर्मचारी

नाम : _____

स्थाई पता : _____

दूरभाष/मोबाइल न. : _____

ई-मेल : _____

कर्मचारी संख्या : _____ विभाग का नाम : _____

दिनांक : (हस्ताक्षर)

अधिष्ठाता/विभागाध्यक्ष की टिप्पणी

.....

.....

दिनांक : अधिष्ठाता/विभागाध्यक्ष

(नाम, हस्ताक्षर एवं मोहर)

कार्यालय प्रयोग हेतु

लॉगिन आईडी : _____ अस्थाई पासवर्ड : _____

लॉगिन प्रदान की तिथि _____ लॉगिन समाप्ति की तिथि : _____

लॉगिन प्रदान करनेवाले अधिकृत अधिकारी का नाम एवं हस्ताक्षर _____

दिनांक : (हस्ताक्षर)

<काटे से काटें>

प्रयोक्ता की प्रतिलिपि

नाम : _____

लॉगिन आईडी : _____ अस्थाई पासवर्ड : _____

नोट : कृपया प्रथम लॉगिन के बाद अपना पासवर्ड अवश्य बदल लें।

नोट : कृपया प्रथम लॉगिन के बाद अपना पासवर्ड अवश्य बदल लें।

इंटरनेट प्रयोग संबंधी निर्देश

- इन्टरनेट का प्रयोग अपने लॉगिन से ही करें।
- अपने लॉगिन का नाम एवं पासवर्ड गुप्त रखें।
- लॉगिन करने के बाद लॉग आउट अवश्य करें।
- किसी तरह की "सामाजिक साईट" देखें एवं "विश्वविद्यालय ई-मेल" किसी को न भेजें अन्यथा उस पर लंबित कार्यवाही की जाएगी और ऐसी स्थिति में लॉगिन समाप्त की जा सकती है।
- अनावश्यक कम्प्यूटर ऑन न करें एवं काम समाप्त होने के पश्चात शट-डाउन अवश्य करें।
- अनुपयोगी विंडोज/मोडिफ्रे को न खोलें/चलाएं।
- यदि आप अपने लॉगिन का प्रयोग नहीं करना चाहते हैं तो इसकी लिखित सूचना तीस दिवस को उपलब्ध दें।
- सहयोग की अपेक्षा के साथ।

सहमति पत्र

मैं, _____ विश्वविद्यालय द्वारा जारी " इन्टरनेट प्रयोग संबंधी निर्देश" से सहमत हूँ। यदि विश्वविद्यालय इंटरनेट प्रयोग करने की नीति में कोई परिवर्तन करता है तो मुझे मान्य होगा।

दिनांक : (आवेदक के हस्ताक्षर)

93
190

2- Internet Use Form for Students of University

इन्टरनेट उपयोग करने हेतु आवेदन-पत्र

छात्रों के लिए

नाम : _____

स्थाई पता : _____

दूरभाष / मोबाइल नं. : _____

ई-मेल : _____

पाठ्यक्रम का नाम : _____ _____

नामांकन संख्या :

विद्यापीठ : _____ विभाग का नाम : _____

सत्र : _____

दिनांक : (हस्ताक्षर)

अधिष्ठाता / विभागाध्यक्ष की टिप्पणी

.....

.....

दिनांक : अधिष्ठाता / विभागाध्यक्ष
(नाम, हस्ताक्षर एवं मोहर)

कार्यालय प्रयोग हेतु

लॉगिन आईडी : _____ अस्थाई पासवर्ड : _____

लॉगिन प्रदान करने की तिथि : _____ लॉगिन समाप्ति की तिथि : _____

लॉगिन प्रदान करने वाले अधिकृत अधिकारी का नाम एवं पदनाम _____

दिनांक : (हस्ताक्षर)

< यहां से काटें >

प्रयोक्ता की प्रतिलिपि

नाम : _____

लॉगिन आईडी : _____ अस्थाई पासवर्ड : _____

नोट : कृपया प्रथम लॉगिन के बाद अपना पासवर्ड अवश्य बदल लें।

इंटरनेट प्रयोग संबंधी निर्देश

- इन्टरनेट का प्रयोग अपने लॉगिन से ही करें।
- अपने लॉगिन का नाम एवं पासवर्ड गुप्त रखें।
- लॉगिन करने के बाद लॉग आउट अवश्य करें।
- किसी तरह की "आपत्तिजनक साईट" न देखें एवं "विवादास्पद ई-मेल" किसी को न भेजें अन्यथा आप पर उचित कार्यवाही की जायेगी और ऐसी स्थिति में लॉगिन समाप्त की जा सकती है।
- अनावश्यक कम्प्यूटर ऑन न करें एवं काम समाप्त होने के पश्चात शट-डाउन अवश्य करें।
- अनुपयोगी वेबसाईट / ऑडियो को न खोलें / डाउनलोड करें।
- यदि आप अपने लॉगिन का प्रयोग नहीं करना चाहते हैं तो इसकी लिखित सूचना तीन दिवस में उपलब्ध कराएं।
- सहयोग के अपेक्षा के साथ।

सहमति पत्र

मैं, _____ विश्वविद्यालय द्वारा जारी "इन्टरनेट प्रयोग संबंधी निर्देश" से सहमत हूँ। यदि विश्वविद्यालय इंटरनेट प्रयोग करने की नीति में कोई परिवर्तन करता है तो मुझे मान्य होगा।

दिनांक : (आवेदक के हस्ताक्षर)

(189) (92)

3. Internet Use Form for Guest Faculty/Guest of University

इन्टरनेट उपयोग हेतु आवेदन-पत्र

अतिथि अध्यापक/अतिथि के लिए

नाम : _____

स्थायी पता : _____

दूरभाष नंबर/मोबाइल नं : _____

ई-मेल : _____

विभाग का नाम : _____

उपाधि :

दिनांक : (हस्ताक्षर)

अधिष्ठाता/विभागाध्यक्ष की टिप्पणी

.....

.....

दिनांक :

अधिष्ठाता/विभागाध्यक्ष

(नाम हस्ताक्षर एवं मोहर)

कार्यालय प्रयोग हेतु

लॉगिन आईडी : _____ अस्थाई पासवर्ड : _____

लॉगिन प्रदान की तिथि : _____ लॉगिन समाप्ति की तिथि : _____

लॉगिन प्रदान कार्यालय प्रतिनिधि अधिकारी का नाम एवं पदनाम : _____

दिनांक (हस्ताक्षर)

<काटे>

प्रयोक्ता की प्रतिलिपि

नाम : _____

लॉगिन आईडी _____ अस्थाई पासवर्ड : _____

इंटरनेट प्रयोग संबंधी निर्देश

- इन्टरनेट का प्रयोग मात्र शैक्षिक है ही करें।
- अपने लॉगिन का नाम एवं पासवर्ड गुप्त रखें।
- लॉगिन करने के बाद लॉग आउट अवश्य करें।
- किसी भी अनधिकृत साईट पर एवं विश्वविद्यालय ई-मेल किसी के द्वारा भेजे अश्लील एवं अवैध सामग्री की जानकारी और ऐसी स्थिति में लॉगिन तत्काल की जा सकती है।
- अनधिकृत कम्प्यूटर और तार को एवं कम्प्यूटर होने के पश्चात् हार्ड-डिस्क्स उपयोग करें।
- अनुपयोगी विडियो, ऑडियो को न खोलें/डाउनलोड करें।
- यदि आप अपने लॉगिन का प्रयोग नहीं करना चाहते हैं तो इसकी लिखित सूचना शीघ्र विभाग को उपलब्ध दें।
- सहयोग की अपेक्षा के साथ।

सहमति पत्र

मैं, _____ विश्वविद्यालय द्वारा जारी "इन्टरनेट प्रयोग संबंधी निर्देश" से सहमत हूँ। यदि विश्वविद्यालय इंटरनेट प्रयोग करने की नीति में कोई परिवर्तन करता है तो मुझे मान्य होगा।

दिनांक : (आवेदक के हस्ताक्षर)

Bhukla

188

4. Email ID – Application Form – Teacher / Officer / Employee

महात्मा गांधी अंतरराष्ट्रीय हिंदी विश्वविद्यालय, वर्धा

शिक्षकों/अधिकारियों/कर्मियों/अनुभागों एवं विभागों के लिए ई-मेल आईडी हेतु आवेदन

आवेदन दिनांक : _____	**विभाग :** _____
संपर्क दूरभाष : _____	**वर्तमान ई-मेल आईडी :** _____

अनुरोधित ई-मेल आईडी का प्रकार : ☐ **शिक्षक** ☐ **अधिकारी** ☐ **अनुभाग** ☐ **विभाग**

अनुरोधित ई-मेल आईडी: .....

(ई-मेल आईडी प्रारूप – Name@hindivishwa.ac.in)

नाम :..... **विभाग** :.....

कार्यभार ग्रहण की तिथि(शिक्षक/अधिकारी/कर्मी के संबंध में) :.....

विश्वविद्यालय में सेवा समाप्ति की तिथि (शिक्षक/अधिकारी/कर्मी के संबंध में):.....

घोषणा (Declaration)

मैं यह घोषित करता/करती हूँ कि इस आवेदन पत्र में दी गई सभी जानकारियाँ सत्य, सही एवं पूर्ण हैं।

मैं यह भी पुष्टि करता/करती हूँ कि मुझे/विभाग/अनुभोग को प्रदत्त ई-मेल आईडी का उपयोग **केवल कार्यालयीन/ शैक्षणिक एवं शोध कार्यों** हेतु ही किया जाएगा।

मैं यह जानता/जानती हूँ कि यह ई-मेल आईडी म गां अं हिं वि द्वारा निर्धारित अवधि तक के लिए होगी।

मैं महात्मा गांधी अंतराष्ट्रीय हिंदी विश्वविद्यालय, वर्धा डोमेन की ई-मेल आईडी के उपयोग से संबंधित वर्तमान एवं भविष्य में लागू होने वाली सभी शर्तों एवं नियमों का पालन करूँगा/करूँगी।

इस आवेदन के साथ मैंने आवश्यक दस्तावेज (यदि लागू हो) संलग्न किया है।

187 30

आवेदक के हस्ताक्षर :.....

<u>विभाग द्वारा अनुमोदन:</u>

(दिनांक मुहर अनिवार्य)

विभागाध्यक्ष / समन्वयक का नाम :..... **हस्ताक्षर :**.....

दिनांक :..... **मुहर :**.....

कृपया ध्यान दें : उपरोक्त अनुरोध को स्वीकृति प्रदान करते समय यह सहमति मानी जाएगी कि यदि कोई शिक्षक/अधिकारी/कर्मी सेवा समाप्ति, स्थानांतरण, सेवा विच्छेद आदि कारणों से विश्वविद्यालय छोड़ता है, तो इसकी सूचना तत्काल ई-मेल द्वारा तकनीकी प्रकोष्ठ **(Technical Cell)** को दी जाएगी।

<u>कुलसचिव द्वारा अनुमोदन</u>

दिनांक :..... हस्ताक्षर:.....

मुहर

<u>केवल कार्यालय उपयोग हेतु</u>

(तकनीकी प्रकोष्ठ द्वारा भरा जाएगा)

ई-मेल आईडी सक्रिय किए जाने की तिथि :	**ई-मेल आईडी निष्क्रिय किए जाने की तिथि :** .....
आधिकारिक हस्ताक्षर :.....	**आधिकारिक हस्ताक्षर :**.....

89
186

5. Email ID – Application Form – Teacher / Officer / Employee

महात्मा गांधी अंतरराष्ट्रीय हिंदी विश्वविद्यालय, वर्धा

स्नातक / स्नातकोत्तर / पीएच.डी के लिए ई-मेल आईडी हेतु आवेदन

आवेदन दिनांक : _____	**विभाग :** _____
संपर्क दूरभाष : _____	**वर्तमान ई-मेल आईडी :** _____

अनुरोधित ई-मेल आईडी का प्रकार : ☐ **स्नातक** ☐ **स्नातकोत्तर** **पीएच.डी** ☐

अनुरोधित ई-मेल आईडी: .....

(ई-मेल आईडी प्रारूप – Name@hindivishwa.ac.in)

नाम :..... **विभाग** :.....

प्रवेश की तिथि (स्नातक / स्नातकोत्तर / पीएच.डी के संबंध में) :.....

विश्वविद्यालय में कोर्स समाप्ति की तिथि (स्नातक / स्नातकोत्तर / पीएच.डी के संबंध में):.....

घोषणा (Declaration)

मैं यह घोषित करता/करती हूँ कि इस आवेदन पत्र में दी गई सभी जानकारियाँ सत्य, सही एवं पूर्ण हैं।

मैं यह भी पुष्टि करता/करती हूँ कि मुझे/विभाग को प्रदत्त ई-मेल आईडी का उपयोग **केवल शैक्षणिक एवं शोध कार्यों** हेतु ही किया जाएगा।

मैं यह जानता/जानती हूँ कि यह ई-मेल आईडी म गां अं हिं वि में द्वारा निर्धारित अवधि तक ही मान्य रहेगी।

मैं महात्मा गांधी अंतराष्ट्रीय हिंदी विश्वविद्यालय, वर्धा डोमेन की ई-मेल आईडी के उपयोग से संबंधित वर्तमान एवं भविष्य में लागू होने वाली सभी शर्तों एवं नियमों का पालन करूँगा/करूँगी।

इस आवेदन के साथ मैंने आवश्यक (यदि लागू हो) दस्तावेज संलग्न किया है।

आवेदक के हस्ताक्षर :.....

<u>विभाग द्वारा अनुमोदन</u>

(दिनांक मुहर अनिवार्य)

विभागाध्यक्ष / समन्वयक का नाम :..... **हस्ताक्षर :**.....

दिनांक :..... **मुहर :**.....

कृपया ध्यान दें : उपरोक्त अनुरोध को स्वीकृति प्रदान करते समय यह सहमति मानी जाएगी कि यदि कोई शिक्षक/अधिकारी/कर्मी सेवा समाप्ति, स्थानांतरण, सेवा विच्छेद आदि कारणों से विश्वविद्यालय छोड़ता है, तो इसकी सूचना तत्काल ई-मेल द्वारा तकनीकी प्रकोष्ठ **(Technical Cell)** को दी जाएगी।

<u>कुलसचिव द्वारा अनुमोदन</u>

दिनांक :.....

हस्ताक्षर:.....

मुहर

<u>केवल कार्यालय उपयोग हेतु</u>

(तकनीकी प्रकोष्ठ द्वारा भरा जाएगा)

ई-मेल आईडी सक्रिय किए जाने की तिथि : ..... **आधिकारिक हस्ताक्षर :**.....	**ई-मेल आईडी निष्क्रिय किए जाने की तिथि :** ..... **आधिकारिक हस्ताक्षर :**.....