



**Bharatiya Vidya  
Bhavan**  
AGARTALA KENDRA

# **BHAVAN'S TRIPURA COLLEGE OF TEACHER EDUCATION**

(Recognised by N.C.T. E. & Affiliated to Tripura University, A Central University)

(Recognized by UGC under Section 2(f) & 12(B) of UGC Act, 1956)

P.O : Bimangarh (Narsingarh), Agartala, West Tripura, PIN - 799 015

Ph. No.: 6033322532, e-mail : bhavanbedc\_trip@rediffmail.com # website : www.btcte.in

**Dr. Rajat Dey**  
Principal

Chairman

F.1(1)/Chairman/Policy/BVB/2021/16

Date: 20-01-2022

## **INFORMATION TECHNOLOGY AND NETWORK POLICY**

### **POLICY STATEMENT**

IT and Network Policies are created and mandatory to implement for maintaining, securing and ensuring legal and appropriate use of college (Bhavan's Tripura College of Teacher Education) IT resources. The policy terms assure a campus community with a high quality, trusted and secure computing environment, with a responsibility of protecting and securing its property interests, data and intellectual property. The college requires people to use its information technology resources in a responsible manner, abiding by all applicable laws, policies, and regulations.

### **REASON FOR POLICY**

The college provides information technology resources to a large and diverse group, including faculty, staff, students, guests and agency. All members of this community are responsible for using these resources in an ethical and respectful manner that protects. College's sensitive information and follows the IT policies. The college must uphold the tenets of academic freedom, while recognizing that protecting information technology and data requires community members to act responsibly when using these resources.

### **SCOPE**

This policy applies to everyone who uses college IT resources, whether physically located on campus or remotely connected. Hence this policy applies to all electronic information stored or transmitted on the college Network and the supporting IT infrastructure and cover all students, faculty, staff – whosoever use the college network.

### **ENTITIES AFFECTED BY THIS POLICY**

All Departments, units and students of the college.

### **WHO SHOULD READ THIS POLICY**

All members of the college community.

### **INTRODUCTION**

All employees, students are provided access to the college computer network, the Internet, smart class and library software facilities. The policy on the IT infrastructure aims to regulate its use by all its authenticated users and the respectable guests. Thus everyone use it appropriately and lawfully for the continuous availability of network and Internet access. The policy when implemented and followed ensures that the electronic information is provided to maintain and uphold the college business and its mission of education, research and service. The priorities for the IT resources can be established and enforced when demand for computing resources exceeds available capacity. For use of college-wide computing resources various priorities are:

  
(DR. RAJAT DEY)  
Principal  
Bhavan's Tripura College of  
Teacher Education  
Narsingarh, Agartala-799015

  
Debashis Chakraborty  
Chairman  
BHARATIYA VIDYA BHAVAN  
AGARTALA KENDRA



- Maximum: Uses that directly support the educational, research and service missions of the college.
- Lowest: Uses that indirectly benefit the education, research and service missions of the college; reasonable and personal communications.
- Prohibited: Amusement activities (game playing, e-trading, E-shopping, social networking, movies and songs, chatting/video chatting or use of VoIP services like Skype etc) unless permitted, use of Torrent and p2p software and all activities in violation of the Indian IT Act.

### PERSONAL RESPONSIBILITY

You agree to abide by the policy terms, by accepting your account password and related information and accessing network or Internet system.

The following are major responsibilities each party has in connection with this policy:

- Department: Implement operational, physical, and technical controls for access, use, transmission, and disposal of college data in compliance with all privacy and security policies, procedures, and guidelines.
- User: Use all (IT) resources and data in a manner that is legal, ethical, and consistent with the mission of education, research, teaching. Abide by all applicable IT policies.

### TERM OF PERMITTED USE

Network, Internet and Smart Class access extends throughout the term of one's employment or stay at the college, provided they do not violate the policy. The college has the right to suspend the access to its IT resources and related services, at any time for technical reasons, policy violations, or other concerns. Internet facility can be accessed by the faculty and staff members using Lan/Wi-fi connectivity. Every faculty/staff room and class room has been provided with cabled network and it is expected that faculty/staff members to use cabled network as preferred network. Access to internet facility, smart class etc. for college is free and is governed by rules and regulations of this policy, however access to social networking and YouTube is allowed in academic time. Internet access can be granted to guests on demand of concerned faculty/staff members. Online access of library books searching through college website has been provided free for faculty/staff member and student.

### PURPOSE AND USE

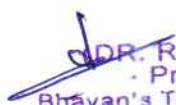
College offers access to its network, Internet, Smart class facility for educational and research purposes only. If one is unsure of the business activity use whether appropriate or not, must consult the server room staff for usage.

### GENERAL RULES

All users must comply with college Rules, Regulations and Policies, cyber laws, IT Act of Government of India and the terms of (applicable) contracts including software licenses while using college IT resources. It may include but not limited to privacy, copyright, trademark, obscenity and child pornography; hacking, cracking and similar activities, Scams and pyramid schemes, the college's Student Code of Conduct etc. Users are responsible for ascertaining the necessary authorizations before using the college IT resources. They are responsible for the activities from their accounts. Under any circumstances, accounts and passwords must not be used by persons other than those to whom they have been assigned by the account administrator. Any detect/suspect of unauthorized use of accounts or resources must be reported to the appropriate account administrator. Users who violate this policy will be subjected to disciplinary action.

### NETIQUETTE RULES

Employees/students must follow the rules of network etiquette (netiquette). That is, they must be polite, follow the organization's electronic writing and content guidelines, and use the network, Computer, Internet, Smart Class, Library book facility legally and appropriately. The college will determine of the materials, files,

  
**DR. RAJAT DEY**  
 Principal  
 Bhavan's Tripura College of  
 Teacher Education  
 Narsingarh, Agartala-799015

  
**Debashis Chakraborty**  
 Chairman  
 BHARATIYA VIDYA BHAVAN  
 AGARTALA KENDRA



information, software, communications, and other contents and activities that are permitted or prohibited, outlined below under violations.

## **VIOLATIONS**

The following activities are considered as violations under the college computer network, Internet and Smart Class use policy. Illegal activities under local, state and national laws any activity that is illegal is a violation of college IT policy. Alleged violations will be referred to the campus Judicial Administrator. In addition, offenders may be investigated and/or prosecuted by the appropriate local, state or national authorities.

- Using, transmitting, viewing or searching for obscene and pornographic materials.
- Conducting unauthorized business on Internet (including share trading).
- Seeking inappropriate, offensive, vulgar, suggestive, abusive, harassing, belligerent, threatening, defamatory actions or misleading language and materials.
- Revealing other persons personal information, or accessing, transmitting, receiving or seeking unauthorized and confidential information.
- Making availability of any materials, whose possession or distribution is illegal.
- Circulating/Broadcasting hate mails, message/announcements or images intended to harm or humiliate others, discrimination or individual attacks on others, or expressing animus towards any person or group by any reason (contest, colour, religion, national origin, gender, sexual orientation or disability) is prohibited. Unauthorized access Computer Systems can have security holes or other breakpoints/weak points that people can use to gain unauthorized access to the system and data. So, unacceptable and unauthorized use of IT resources and data includes (but not limited to) the following:
- Any attempt to acquire or using passwords of others; attempt to use or using the computer accounts of others;
- Accessing others folders, files, work, network (unless permitted), or computer, and interrupting communications of others.
- Any kind of transmit/Download of copyright materials without having consent from the copyright holder; one should assume all materials are confined to copyright laws except any explicit authorization to use them is provided.
- Use of social networking sites unless permitted.
- Watching/downloading movies and songs.
- Making college IT resources available to individuals not related to college without approval of an authorized college official.
- The interception of communications by parties not explicitly intended to receive them without approval of an authorized college official.
- Unauthorized duplicity or use of licensed computer software.
- Any unauthorized access, control, or broadcast of electronic information or data that is confidential under the college's policies.
- Connecting your machine to any wireless network other than the designated network while on-campus, unless authorized.
- Providing substances prohibited by the universities employment policy/IPR Policy or the Employee Rules regulations.
- Any attempt to alter any college computing or networking resources without taking permission or beyond individual's level of authorization; Unauthorized wiring, including attempts to create



unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services.

- Maliciously accessing, altering, deleting, damaging or destroying any computer system, network, program or data. Examples are:
  - Changing or deleting another user's account/password of another user,
  - Using an unauthorized account, damaging or deleting college files
  - Altering the college network system, mishandling, damaging or tampering with computer equipment, software or settings.

## MAILING VIOLATIONS

Flooding someone with numerous/ large e-mails or with suspicious content is to disrupt them or the related group, which causes problems not only for the local system but also disrupts service for thousands of other innocent bystanders. Such activities include, but are not limited to the following:

- Using the college e-mail system to relay personal e-mails.
- Engaging in spam activities (i.e., sending unsolicited electronic communications to large groups of individuals at the same time) or sending e-mail chain letters.
- Sending hate mail, statements or images intended to injure or humiliate others, threats, personal attacks on others or statements expressing animus towards any person or group by reason of race, colour, religion, national origin, gender, sexual orientation or disability is prohibited. This includes any such messages transmitted via e-mail, instant messaging or any other electronic means which rely on the college network for transmission.
- Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts; Unauthorized scanning of networks for security vulnerabilities.
- Wasting the computer resources, printer toner or paper, sending electronic chain letters, e-mail copies to nonessential readers, e-mails to group lists unless it is appropriate for everyone on a list to receive the e-mail, and organization wide e-mails without your supervisor's permission.

## FORGERY

- Altering electronic communications to hide your identity or to harm some other person, even ones that are intended as pranks or jokes are considered as violations. A few of them includes:
- Alteration of the content of a message originating from another person or computer with intent to deceive.
- Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication.
- Using the college network or computer resources for commercial purposes or personal gain.
- Misrepresenting oneself as another user by using their ID's.

## SECURITY AND NETWORK BREACH

Installing software on any college owned equipment (pirated or freeware/shareware). Using software that is not licensed or approved by the college.

- Attempting to monitor or capture BSNL network traffic.
- Intentionally compromising the privacy or security of electronic information; and intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).

  
**DR. RAJAT DEY**  
Principal  
Bhavan's Tripura College of  
Teacher Education  
Moranagarh, Agartala-799015


  
**Debashis Chakraborty**  
Chairman  
BHARATIYA VIDYA BHAVAN  
AGARTALA KENDRA



- Attempting to security of various software or other security measures placed on college (BSNL) network systems or computers.
- Engaging in illegal activities, violating the Employee Codes/Rules/regulations, or encouraging others to do so.
- Circumventing network bandwidth restrictions by altering the network address.
- Mishandling, damaging or tampering with computer equipment, software or settings.
- Disrupting or attempting to disrupt network traffic or attempting to overload or crash the college network and attached systems.
- Maintains insecure passwords on IT devices attached to the network
- Attaching misconfigured IT devices to the network.
- Compromising an IT device, use of an application or computing system attached to the network.
- To perform network or system scans on resources not authorized by the IT security department.

## GUIDE LINES


1. **NETWORK REGISTRY:** College is concerned with creating and maintaining a registry service with Next Education India Pvt. Ltd for Smart Class, Digilib for Library facility, BSNL Internet for other uses. The said service maintains an updated database with current records of all the devices connected to the central network, including the wireless connections. Authentication to IT resources, to protect the IT resources from unauthorized use, college must protect them and support regulations governing the privacy and security of sensitive data by the use of electronic identifiers and secure passwords to control access.
2. **DATA BACKUP:** Google drive, which is a complete Data management solution. Following steps will be adhered by all while using the Google drive, external hard disk pan drive.
3. **CONFIDENTIAL INFORMATION:** Employees may have access to confidential information about the college, once written approval is granted. With the approval of management, employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mail must be marked "confidential." When in doubt, does not use e-mail to communicate confidential material. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.
4. **PRIVACY:** Network, Website and Internet access is provided as a tool to accomplish the organization's strategic goals and objectives. The college reserves the right to monitor, inspect, copy, review, and store at any time and without prior information any and all network and Internet use, as well as any and all materials, files, information, software, communications, and other content transmitted, received, or stored in connection with this use. All such information, content, and files are the property of the college.
5. **NON COMPLIANCE:** The use of the computer network, the Internet and Library software is a privilege, not a right. Violation of this policy, at the minimum will lead to disciplinary action. Policy breaches include violating the above provisions and failing to report violations by other users. Permitting another person to use your account or password to access the network or the Internet including, but not limited to, someone whose access has been denied or terminated is a violation of policy. In case another user violates this policy using ones account, the account holder will be held responsible and both will be subject to disciplinary/administrative action. Criminal violations may lead to criminal or civil prosecution.

  
(DR. RAJAT DEY)  
Principal  
Bhavan's Tripura College of  
Teacher Education  
Narsingari, Agartala-799015

  
Debashis Chakraborty  
Chairman  
BHARATIYA VIDYA BHAVAN  
AGARTALA KENDRA




6. **SECURITY MEASURES:** Physical security is used to protect resources such as keys, doors, and/or rooms maintained to the level of security commensurate with the value of the resources stored in those locations.
7. **ADMINISTRATIVE SECURITY:** To protect resources such as -
- Full implementation of the most current authentication and authorization technologies.
  - Most recently tested and approved software patches available.
  - Most contemporary and available security configurations.
  - Most contemporary and available virus protection.
  - Configuration of secure passwords on all IT devices
8. **REVISION:** This policy may be modified as deemed appropriate by the college. Users are encouraged to periodically review the policy as posted on the college's website page.
9. **DISCLAIMER:** Security is neither perfect nor permanent. This is even more true for Information and IT infrastructure where change is the only constant - systems change, requirements change, new bugs are discovered, new vulnerabilities are disclosed, new threats arise, old vulnerabilities take new forms - all this as the information and the equipment go through their lifecycles from creation and use to destruction, and from great value for the organization to none. In this Dynamic environment, this document attempts to bring some long-lasting order and balance. Owing to the very nature of its subject, this document, too, is neither perfect nor permanent. The document must necessarily be periodically updated for it to remain effective.



Dr. Rajat Dey  
Principal  
BTCTE, Narsingarh

(DR. RAJAT DEY)  
Principal  
Bhavan's Tripura College of  
Teacher Education  
Narsingarh, Agartala-799015



Shri. Debashis Chakraborty  
Chairman  
BVB, Agartala Kendra

Debashis Chakraborty  
Chairman  
BHARATIYA VIDYA BHAVAN  
AGARTALA KENDRA