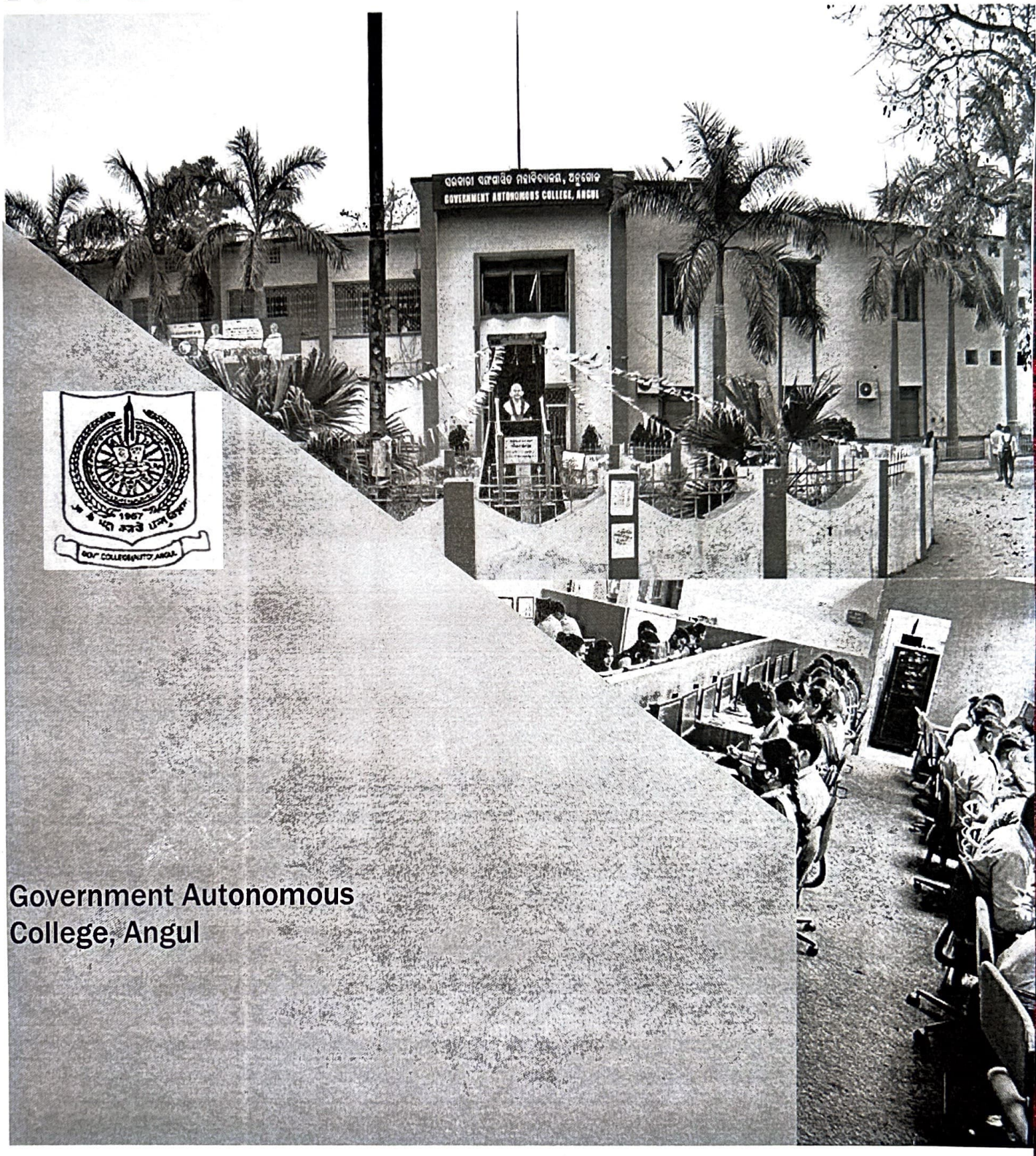
IT POLICY



Government Autonomous College, Angul

GOVERNMENT AUTONOMOUS COLLEGE, ANGUL

IT POLICY

PREAMBLE

The Government Autonomous College, Angul Information Technology (IT) Policy sets forth the policies that govern the responsible usage of all users of the college's information technology resources. Every member of college is expected to be familiar with and adhere to this policy. Users of the campus network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others.

For the purpose of this policy, the term 'IT Resources' includes all College owned, licensed, or managed hardware and software, and use of the College network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

APPLICABILITY

This document establishes specific requirements for the use of all IT resources at college. This policy applies to all users of computing resources owned or managed by college. Individuals covered by the policy include College faculty and guest faculty, staff, students, alumni, guests, external individuals, and any other entity that fall under the management of college accessing network services via computing facilities of the College.

OBJECTIVES

College IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the college on the campus. Misuse of these resources can result in unwanted risk and liabilities for the college. It is, therefore, expected that these resources are used primarily for college related purposes and in a lawful and ethical way.

- This policy establishes College-wide strategies and responsibilities for protecting the Confidentiality, Integrity and Availability of the information assets that are accessed, created, managed and/or controlled by the college.
- This policy to ensure that the IT resources protects the official e-identity (allocated by the college) of an individual
- To ensure that all the users of the College are responsible for adhering to the procedures governing the implementation of this Policy document and any other matter incidental to those rules
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

NEED OF IT POLICY

Basically, this HEI's IT policy is to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the college on the campus.

This policy establishes College-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the College.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information Intranet& Internet services have become most important resources in educational institutions & research organizations.

Realizing the importance of these services, Govt. Autonomous College, Angul took initiative and established basic network infrastructure in the premise of the College.

Now, the College has six network connections from two vendors JIO and BSNL covering more than twenty departments and administrative departments across the campus.

Details of LAN Connections

ISP Details	Place of Installation	Configuration
BSNL-Fibre Premium Plus-296079	IQAC Cell	200 Mbps
BSNL-Fibre Premium Plus-296080	Autonomous Section	200 Mbps
BSNL-Fibre Premium Plus-296081	Computer Science	200 Mbps
BSNL-Fibre Premium Plus-296082	Office, SAMS Admission	200 Mbps
BSNL 200 Mbps dedicated ILL in OFC	10 LAN ports in Offices	200 Mbps

Details of Wifi in Campus

ISP Details	Place of Installation	Configuration
JIO NET	Whole Campus	
BSNL 200 Mbps dedicated ILL in OFC	Whole Campus	**200 Mbps**

All the faculty members using this network for teaching and learning. Govt. Autonomous College, Angul is getting its Internet band width from BSNL and JIO. There are two types of connection from BSNL with four connection of bandwidth 200 Mbps covering Computer Science Laboratory, SAMS (Admission and Academic Section), Principals Office (includes Accounts Section, Establishment Section, and Library), IQAC Section, and Examination Section. Another connection from BSNL covering all departments and sections of the college of bandwidth 200 mbps.

There are two wireless internet connections (WiFi) for staff and students one from Jio, BSNL and another from BSNL of 200 Mbps.

An effective security policy is as necessary to a good information security program as a solid foundation to the building. Hence, GOVT. AUTONOMOUS COLLEGE, ANGUL also is

proposing to have its own IT Policy that works as guidelines for using the College's computing facilities including computer hardware, software, email, information resources, intranet, and Internet access facilities, collectively called "Information Technology (IT)."

Hence, this document tries to propose some IT policies and guidelines that would be relevant in the context of this College. While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing requirements of the IT user community, and operating procedures.

Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of college community to understand how College policy applies to some of the significant areas and to bring conformance with stated policies.

ROLES AND RESPONSIBILITIES

The following roles and responsibilities are envisaged from each entity respectively.

- College shall implement appropriate controls to ensure compliance with this policy by their users. IT Section or the Officer In-charge appointed by Principal shall be the primary Implementing Agency and shall provide necessary support in this regard.
- Use College's IT resources for those activities that are consistent with the academic, research and public service mission of the College and are not "Prohibited Activities".
- All users shall comply to existing national, state, and other applicable laws.
- Abide by existing telecommunications and networking laws and regulations.
- Follow copyright laws regarding protected commercial software or intellectual property.
- As a member of the College community, College provides use of scholarly and/or work-related tools, including access to the Library, certain computer systems, servers, software and databases and the Internet. It is expected from College Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources.
- Users of College shall not install any network/security device on the network without consultation with the Implementing Agency.
- It is the responsibility of the College Community to know the regulations and policies of the College that applies to appropriate use of the technologies and resources. College Community is responsible for exercising good judgment in the use of the available technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
- As a representative of the College community, everyone is expected to respect and uphold the College's good name and reputation in any activities related to use of ICT communications within and outside the College.
- Competent Authority of College should ensure proper dissemination of this policy.

ACCEPTABLE USE

- An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account, or attempt to capture or guess other users' passwords.
- A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software and hardware. Therefore, he/she is accountable to the College for all use of such resources. As an authorized College user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of college or a personal computer that is connected to the College campus through the Local Area Network (LAN).
- The College is bound by its End User License Agreement (EULA), respecting certain third-party resources; a user is expected to comply with all such agreements when using such resources.
- Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
- No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- The users shall not send, view, or download fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable law or College policy. Contributing to the creation of a hostile academic or work environment is prohibited.
- Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file sharing using the College's information resources is a violation of this policy.
- The College IT resources shall not be used for any commercial and promotional purposes, through advertisements, solicitations or any other message passing medium, except as permitted under College rules.
- Users must comply with the policies and guidelines for any specific set of resources to which he/she has been granted access.
- When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

PRIVACY AND PERSONAL RIGHTS

1. All users of the College's IT resources are expected to respect the privacy and personal rights of others.
2. Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
3. While the College does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.

PRIVACY IN EMAIL

While every effort is made to ensure the privacy of college email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct College business, there may be instances when the College, based on

approval from competent authority, reserves and retains the right to access and inspect stored information with the consent of the user.

USER COMPLIANCE

When an individual uses college's IT resources, and accepts any college issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of college and adapt to those changes as necessary from time to time.

The College shall endeavour to ensure fair implementation of this policy to meet with the objectives of its formation. The responsibility of the management of operational aspects of IT resources is as per the hierarchical flow of the College governance structure.

The respective Heads of the sections shall be responsible for compliance with all college IT policies relating to the use/ownership of information resources, keeping in mind the Vision and Mission of the College.

WEBSITE & TECHNICAL COMMITTEE at College Level shall coordinate various activities related to the adherence of the IT Policies in association with the IT Administrator of the college.

ACCESS TO THE NETWORK

- Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.
- Wireless client systems and wireless devices shall not be allowed to connect to the College's wireless access points without due authentication.
- To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.
- Implementing Agency (IA) may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.
- Implementing Agency (IA) may also block content which, in the opinion of the College, is inappropriate or may adversely affect the productivity of the users.

USE OF IT DEVICES ISSUED BY COLLEGE

IT devices issued by the College to a user shall be primarily used for academic, research and any other College related purposes and in a lawful and ethical way. This covers use of desktops, laptops, portable devices, external storage media and peripherals devices such as projectors, Wi-Fi, copiers, printers, and scanners etc.

ENFORCEMENT

- This policy is applicable to all the users of College. It is mandatory for all users to adhere to the provisions of this policy.

- Each entity of College shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.

DEACTIVATION

- In case of any threat to security of College's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.
- Subsequent to such deactivation, the concerned user and the competent authority of the College shall be informed.

AUDIT OF COLLEGE NETWORK INFRASTRUCTURE

The security audit of NIC network infrastructure shall be conducted periodically by an organization approved by the College. The security audit of the HEI's website shall be done by an authorized agency or NIC, the host of the website.

DISPOSAL OF ICT EQUIPMENT

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the College as per govt. norms.

VIOLATION OF THE POLICY

Any violation of the basic objective and areas mentioned in the IT policies of college shall be considered as a violation and as a misconduct and gross misconduct under college Rules.

IMPLEMENTATION OF POLICY

For implementation of this policy, the college will decide necessary rules from time to time.

REVIEW AND MONITORING

Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee (ICT) with the approval of the Competent Authority of the College.

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

Review of the policy document shall be done by a committee chaired by Principal & Chairman IQAC of the College .The other members of the committee shall comprise of all Bursars ,Website & Technical Committee, Head of the departments and other members nominated by Principal.

OFFICER-IN-CHARGE 19.07.24

19/7/2024
PRINCIPAL
Principal
Govt. Auto. College, Angul