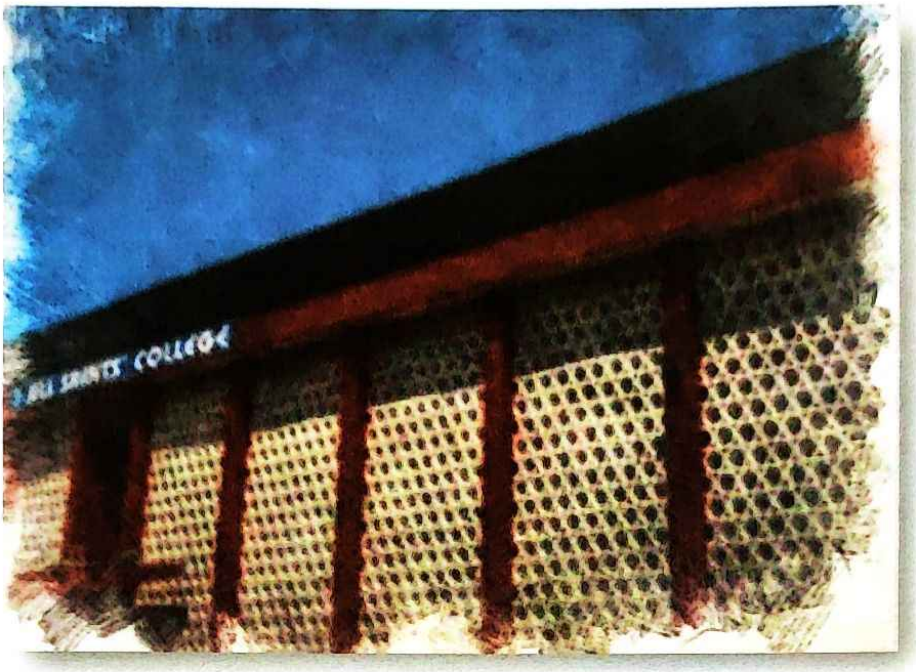
POLICY DOCUMENT



ALL SAINTS' COLLEGE

THIRUVANANTHAPURAM-695007

Re-accredited with 'A+' Grade by NAAC

www.allsaintscollege.ac.in, allsaintscolegeasc@gmail.com

POLICY NAME	IT				
APPLIES TO					
MANAGEMENT	✓	FACULTY	✓	NON-TEACHING STAFF	✓
STUDENTS	✓	PARENT/GUARDIAN	✓	STAKEHOLDERS	✗

Updated on 05.09.2023

PRINCIPAL
All Saint's College
Thiruvananthapuram

ALL SAINTS' COLLEGE
TRIVANDRUM-7, S.INDIA

MANAGER
ALL SAINTS' COLLEGE, TVPM-7

Policy:

1. Access

Most of the information technology resources of the College are accessible to members of the College community. Some resources are also accessible to the public. Access to certain resources may require authorization by an academic or administrative department head who will also provide adequate orientation and training for the appropriate use of such resources. Users are not to attempt to access, search or copy information without the proper authorization.

A user's network identifier and passphrase provide access to information technology resources. In some cases, this includes authorized access to restricted information. A user's network passphrase is not to be shared with anyone, and its confidentiality is to be strictly maintained. Users will be held accountable for all actions performed under their network identifier, including those performed by other individuals as a result of user negligence in protecting their network passphrase. If a user's passphrase is compromised, the user must change the passphrase immediately. Students, faculty, and staff are required to change their passphrases every 365 days. No one is to use the information technology resources through another individual's network identifier, either with or without permission. Active sessions are not to be left unattended. Providing false or misleading information in order to gain access to information technology resources is prohibited.

2.Confidentiality

Academic, financial and personnel records of the College are considered confidential whether or not they exist in computerized form. Every effort will be made to limit access to those records only to authorized individuals. The College may be compelled to release confidential records to comply with legal obligations. All users with access to confidential data are to safeguard the accuracy, integrity and confidentiality of that data by taking all necessary precautions and following established office procedures to ensure that no unauthorized disclosure of confidential data occurs.

3.Privacy

The College conducts monitoring of information technology resources in order to protect the confidentiality, integrity, and availability of these resources, as well as to comply with laws, industry regulations, and licensing requirements. The College will not conduct targeted monitoring of an individual's electronic data, software and communications as a routine matter, however, the College reserves the right to monitor, access and to disclose the contents of an individual's electronic data, software and communications when a legitimate need exists. The reasons for such monitoring, access and disclosure include, but are not limited to, investigations of serious violations of College policies or unlawful activities.

Users should note that all network files are regularly copied to backups and stored for indefinite periods in off-site locations. In such instances, user deletion of an electronic file may not delete a network copy of that file. It is a violation of College policy for authorized users to access confidential files of others without a legitimate academic or administrative purpose.

4.Copyright

The College respects the ownership of intellectual material governed by copyright laws. All members of the College community are to comply with the copyright laws and the provisions of the licensing agreements that apply to software, printed and electronic materials, graphics, photographs, multimedia, and all other information technology resources licensed and/or purchased by the College or accessible over network resources provided by the College. Individual author, publisher, patent holder and manufacturer agreements are to be reviewed for specific stipulations.

5. Web Use

A significant portion of the College's information technology resources is its web site. Faculty, staff and students authorized to publish on the web must comply with prevalent college council decisions.

6. System Integrity and Protection

The integrity and protection of the College's information technology resources are integral to an efficient and high-performance network. Any activity that compromises the integrity or protection of the system is prohibited. Such activities include but are not limited to:

- Creation, importation or exportation of destructive code, such as a virus
- Degradation of system performance, including the creation of unnecessary processes or excessive printing
- Unauthorized use of mass e-mail
- Propagation of chain e-mail
- Failure to provide adequate physical security for information technology resources

7. Prohibited Uses of Information Technology Resources

Faculty, staff and students are encouraged to make full use of the College's information technology resources. Such use, however, is not without limitations. Any activity that violates College policy or any local, state or federal law is prohibited. The following uses are also proscribed:

- Soliciting sales, advertising or managing a private business
- Impersonating other individuals or concealing one's identity in electronic communication
- Viewing offensive or objectionable material at publicly accessible stations
- Posting illegal, offensive or objectionable material on the College website

Communications from members of the College community are to reflect mutual respect and civility. Obscene or intolerant language, as well as offensive images,

clearly violate these standards and are considered inappropriate for electronic and all other forms of discourse among members of the College community. The determination of what is obscene, offensive or intolerant is within the sole discretion of the College. Users should note that College information technology resources may be accessed by minors.

8. Reporting Suspected Violations

Suspected violations of this policy are to be reported to the IQAC Co-ordinator. Depending on the nature of the violation, the IQAC Co-ordinator may refer the matter to the relevant academic or administrative vice president. If a suspected violation is reported instead to a supervisor, chairperson, director, dean or other responsible person, that person is to report the instance to the IQAC Co-ordinator.

The College will consider the intent, effect, and seriousness of the incident in levying sanctions for violations of this policy. Any person who engages in any prohibited activity as described above may be subject to disciplinary action, including the loss of computer privileges and/or dismissal from the College, and to criminal prosecution under the applicable state and/or federal laws.

ALL SAINTS' COLLEGE TRIVANDRUM-7. S.INDIA

OFFICE OF THE MANAGER ALL SAINTS' COLLLEGE