
# Information Technology Policy Handbook

Version 1.0

Release Date: 9-June-2021

Salesian College

UGC Certified College of Excellence
Re-accredited by NAAC (3rd Cycle) with Grade 'A'
Affiliated to University of North Bengal
Post Office Box: 73, SILIGURI- 734 001

https://www.salesiancollege.ac.in

| | |
|---|---|
| Policy Owner | Salesian College |
| Contact | IT Department Head |
| Policy Number | |
| Approved By | The Principal |
| Date Approved | |
| Last Reviewed | |
| Related Documents | |

# Purpose

The Salesian College recognizes the vital role Information Technology plays in the Institution's missions and related administrative activities as well as the importance in an academic environment of protecting information in all forms. As more information is used and shared in a digital format by students, faculty and staff, both within and outside the Institution, an increased effort must be made to protect the information and the technology resources that support it. Increased protection of our information and Information Technology Resources to assure the usability and availability of those Resources is the primary purpose of this Policy. The Policy also addresses privacy and usage of those who access Institution's Information Technology Resources.

# Contents

# Section I - Introduction

The Information Technology Department, consisting of the Tech Team and Salesian Tech, is the nucleus of computing and technology at Salesian College. IT Department manages and maintains the Institution's ERP System, LMS System, Web Sites, Salesian Radio, Salesian TV, Computer Labs, Classroom Technology, Office Computers, Campus Network, Institution collaboration platforms like Google Suite and the Institutional social media sites like Facebook account, Twitter and Instagram account and YouTube channels. IT Department's mission is to fulfil the computing needs of students, faculty, and staff; to provide reliable technology support to the institution in its mission of enabling the youth in Higher Education.

Information is a vital Institution asset and requires protection from unauthorized access, modification, disclosure or destruction. Maintaining the security, confidentiality, integrity, and availability of information stored in the Institution's electronic systems and in paper form is a responsibility shared by all users.

## General Principles

### Academic Freedom

Academic freedom is a fundamental value. This Policy will be administered in a manner that supports the principle of academic freedom.

### Stewardship of Information and Technology Resources

All members of the Institution have responsibility to protect Institutional resources for which they have access or custodianship. Members are accountable for their access to and use of Institutional resources.

An employee of the institution has access to various sources and types of information and supporting technologies in order to complete the responsibilities of his/her job. Use of information and technology that support electronic information is governed by local, state, and national policies. Much of the information the Institution keeps about individual students, alumni and employees is considered sensitive, confidential and private, and must be handled accordingly.

This document establishes guidelines to govern the access, release and use of Institution's information resources. To receive access to the Institution's electronic information resources, one must familiarise oneself with the standards and policies related to appropriate handling and use of the data, and one should sign an access and compliance form indicating his/her understanding and acceptance of the Institution's policies. Staff members who misuse or abuse their access to information and technology resources are subject to disciplinary action, including dismissal.

As a steward of information resources, a member's fundamental responsibilities include:

- Understanding and abiding by the principles of data access, privacy and management.
- Handling all Institution data according to the data management policies, regardless of whether the data relate to one's Department or to another Department.
- Learning, following and upholding the laws and policies that protect information from unauthorized access, alteration, disclosure or destruction.
- Storing information one obtains under secure conditions and making every reasonable effort to maintain the privacy and confidentiality of the data.
- Disposing of confidential data, when one is done using them, in an appropriate manner.

- Interpreting and presenting data one accesses in a professional, accurate manner.
- Prior to sharing data with others, ensuring that the recipient is authorized to access/ view such information and understands his/her responsibility as a user.
- Establishing procedures and practices for purging and archiving data, taking into account requirements for maintaining, preserving, securing and accessing historical data.
- Collecting data with careful consideration to the amount of information needed to serve a defined, legitimate and current institutional purpose.
- Using data only for the purpose for which they were collected.
- Sharing data appropriately with other members of the Institution to avoid unnecessary duplication.

### Personal Use and Privacy

The Institution recognizes that students, faculty and staff have reasonable expectations of privacy in their uses of Information Technology Resources. However, rights to privacy are constrained in the Institution environment because
(1) the Institution owns and supplies these Information Technology Resources to its faculty, staff and students fundamentally for the purpose of accomplishing its academic and educative missions,
(2) the Information Technology Resources contains many closely shared environments and resources and the rights of other users must be taken into account and
(3) legal and ethical restrictions apply. Individuals may have access to unconstrained use through private or commercial systems located at their residence or elsewhere. Resources or systems owned and maintained by the Institution for the benefit of the academic community are primarily intended for use for the Institution, and not for personal or business communications.

## Scope

### People to whom the Policies apply

Policies described here apply to everyone who accesses Salesian College Information Technology Resources, whether affiliated with the Institution or not; whether on campus or from remote locations, including but not limited to students, faculty, staff, contractors, consultants, temporary employees, guests, and volunteers. By accessing Salesian College Information Technology Resources, the user agrees to comply with the policies.

### Information Technology Resources

Information Technology Resources, for purposes of this document, include, but are not limited to, Institution-owned transmission lines, networks, wireless networks, servers, exchanges, internet connections, terminals, applications, and personal computers; those owned by the Institution and those used by the Institution under license or contract - including but not limited to - information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems. Information Technology Resources also include, but is not limited to, personal computers, servers, wireless networks and other devices not owned by the Institution but intentionally connected to the Institution-owned Information Technology Resources (other than temporary legitimate access via the world wide web access) while so connected.

# Section II - Privacy

## Access Restrictions for Personal Communications

The Institution will not, without user permission, monitor, review or otherwise access Personal Communications (defined below) sent or received (e.g., email), created or stored on Information Technology Resources, except pursuant to the Access Procedures set forth here under, which permits access when determined reasonable by a senior administrative officer or for Information Technology Management. The reasons for which access to Personal Communications can be granted include, but not are limited to, the following circumstances:

- To investigate or prevent a violation of law or Institution Policy;
- To protect safety or to provide assurance to the Institution or to other regulators or law enforcement authorities that harm has not occurred to students or others;
- To minimize or stop computer activity that interferes with the Institution's network or other computer operations;
- To comply with a subpoena, warrant, court order or similar legal process, including a discovery request or a litigation stay order issued by or investigation undertaken by the Management in connection with a potential claim in anticipation of litigation; OR
- When the user is unwilling, unable or unavailable to consent, to access Personal Communications needed by another employee in order to fulfil a teaching, research, or other legitimate Institution function.

The access restrictions and approval process do not apply to electronic communications and records supporting Institutional Communications when accessed by authorized individuals for the purpose of carrying out Institutional Business. The approval process described below applies only if access is sought to Personal Communications.

"Personal Communications" are limited to non-Institution related personal emails, documents and correspondence. All other emails, documents, and correspondence prepared by a faculty member, student or employee in connection with his or her job responsibilities are defined as "Institutional Communications" and may be accessed as needed for the purpose of carrying out Institutional Business without seeking prior approval.

"Institutional Business" refers to the Institution's activities and functions, including, but not limited to, administrative functions in the areas of teaching, student life, NCC, NSS, EDC, ENACTUS, Alumni, associations and collaborations, IGNOU and University of North Bengal, institution driven research, as well as supportive administrative services.

## Access Procedures

### A. Institutional Communications

Institutional Communications may be accessed for the purpose of carrying out Institutional Business by individuals with authority to deal with communications related to their subject matter without prior permission from a higher official.

It is understood in the environment of Information Technology Resources that there may not always be a physical separation of electronic records between Institutional Business and Personal Communications. If material is found during a legitimate search for Institutional Communications that indicate a potential violation in Personal Communications of Institutional policy or illegal use, the individual(s) involved in the search should halt the search, secure the relevant Information Technology Resources and seek

permission to access the Personal Communications under the procedure set forth under Personal Communications. Users are reminded of the General Principle in Section I that resources and systems owned and maintained by the Institution are intended for use for the Institution and not for personal or business communications. Individuals who want unconstrained use and privacy should use private or commercial systems located at their residence or elsewhere - not the College IT Resources. Individuals using Institutional IT Resources should recognize that complete privacy is not assured and should refrain from creating or keeping on Institutional IT Resources communications that they wish to keep private.

## B. Personal Communications

With respect to personal communications, anyone seeking access to Electronic Files of an Employee or Student without user consent must first present to a senior official (Principal, Vice Principal/s, the Administrator, or the Dean/s) reasonable cause for gaining such access. (See section I for examples of reasonable cause). If the initiator of the request is a senior Institution Official, the request must be approved by another senior Institution Official. If the initiator of the request is the Principal, the request must be brought to the notice of the Governing Body. An individual cannot initiate a request for access and also be part of the decision-making process. Permission should generally be sought from the official in charge of the Department relevant to the search if that official is available.

In requesting access to Personal Communications without user consent, the person seeking access should provide to the Official relevant information available to support the reasonable cause. The request regarding access should be in writing (email is preferable) to the Official with a copy sent to the Vice Principal/s. The decision of the Official must be in writing (email is preferable) directed to the person requesting access with a copy to the Vice Principal and, if access is granted, a copy to the Information Technology team member who will oversee access.

**a. Preservation and Internal Review of Electronic Files by the Office of Administrator**

1. IT Department will create and maintain for five years from completion of the related investigation a record of all requests to preserve, duplicate and/or provide to the Office of Administrator the contents of electronic files created or maintained by any Employee or Student of the Institution. The information captured on the log will include the identity of the individual approving the request and specify the action taken by IT Department in response to the request.

2. All requests to IT Department to preserve, duplicate or provide Electronic Files will be responded to in strict compliance with this Policy.

3. When Electronic Files are provided for review to the Office of Administrator, notice (with sufficient specificity to describe the files subject to review) to the Employee or Student who created or maintains the electronic file(s) at issue will be provided by the Office of Administrator as soon as practicable unless notice should be delayed at the direction of law enforcement or the Office of Administrator. Any decision of the Office of Administrator to delay disclosure must be based on preservation of confidentiality of an active investigation and any delay in notifying such Employee or Student that extends beyond three weeks will require the approval of the Principal.

4. Electronic files that are preserved, duplicated or provided to the Office of Administrator will be retained on a secure server or dedicated digital media maintained by IT Department and will have the same level of security as other Institution email systems.

5. IT Department will create and preserve an exact copy of the electronic files provided to the Office of Administrator for a period of five years.

**b. Distribution of Electronic Files beyond the Office of Administrator**

1. If the Office of Administrator determines that access to electronic files must extend beyond the Office of Administrator, consent of the Principal shall be obtained before access is granted. Upon Principal's

consent, IT Department will create an exact copy of any electronic files that will be shared or provided. The exact copy of the files and the documentation of the approval process will be retained on a secure server or dedicated digital media maintained by IT Department for five years, and will have the same level of security as other Institutional email systems.

2. Upon Principal's consent, the Office of Administrator will notify the individual(s) who created or maintained the electronic files. Such notice will be provided as soon as practicable unless, at the direction of law enforcement, the Department of Public Safety or the Office of Administrator, notice should be delayed. Any decision of the Office of Administrator to delay disclosure must be based on preservation of confidentiality of an active investigation and any delay in notifying such Employee that extends beyond three weeks will require the approval of the Principal.

3. This section does not apply to electronic files shared with outside counsel or litigants, administrative or governmental agencies, or courts of law. Nothing in this section is meant to restrict the Institution's legal and the Office of Administrator's ethical obligations to comply with governmental investigations, laws or rules governing discovery or disclosure in legal or administrative actions, or to comply with any court order or subpoena for records.

**c. Oversight of Review and Distribution of Electronic Files**

Oversight of this activity will be the responsibility of the Institution IT Policy Committee and shall include faculty representatives. Institution IT will produce an annual report to the Institution IT Policy Committee, showing aggregated and de-identified requests received since the last report to preserve, duplicate and/or provide the contents of electronic files created or maintained by employees.

The Office of Administrator will produce an annual aggregated and de-identified report of any disclosures made as described in Paragraph B (1), and those disclosures will be retrospectively reviewed by the IT Policy Committee. In the event of a disclosure of Electronic Files as described in Paragraph B (1) created or maintained by a Student, the IT Policy Committee will include a student as an ad hoc member for the limited purpose of reviewing that disclosure. Faculty body executive leadership may request reports and clarification from the Secretary of the University IT policy committee, and such reports will maintain respect for the privacy concerns of the individual.

Some employees, to perform their assigned duties, must have special privileges to access hardware and software, including specific files. Such employees are expected to abide strictly by this Policy, and are subject to discipline, including termination, for violating it.

In emergency situations in order to prevent destruction of equipment or data, it may be necessary for the Institution to seize or otherwise secure computers or other information technology pending initiation under this Policy concerning access to the information contained therein. The Institution reserves this right with respect to information technology governed by this Policy.

## C. Information Technology Management and Audit

The Institution may use mechanisms to manage the information technology operations, including (but not limited to) spam and virus detection and elimination; limitation of network volume or blockage of access to specific file types or sites; or restriction of access to sites that present a security risk to the Institution's systems or experience high volumes of network traffic unrelated to the academic missions of the Institution. Use of such mechanisms must be approved by Information Technology Head or any other person designated by the Administrator and must be consistent with legitimate Institutional business needs. It may be necessary for the Office of Administrator or the University's outside auditors in the course of an audit to access Information Technology Resources and information stored thereon. Audits are authorized by the Governing Board or by the Principal and are governed by protocols that protect unnecessary disclosure of information.

# Section III – Data Classification and Access Restrictions

Access to information owned by the Institution is generally broadly consistent with the concept of academic freedom and the open nature of the institution. However, there are types of information where access must be restricted and caution needed in handling and storing the information.

## I. Legally Restricted Information

The disclosure and use of the following types of information is restricted by law.

A. Aadhar Numbers

B. Student Information

C. Financial Account, Credit and Debit Card Information

D. Employee Personnel Records

Access and Use: Legally Restricted Information must be stored, used and disclosed to others only on a need to know basis to permit the individual faculty or staff member to perform their Institutional functions for which the information was acquired and for which it is maintained. Access to legally restricted information must be carefully safe-guarded.

Protection of Legally Restricted Information from disclosure to or unauthorized access by anyone who does not have a legitimate need to access the information to comply with requirements of the law or to carry on necessary Institutional functions is a primary responsibility of the Custodian.

Alternatives to using Legally Restricted Information should be identified and used whenever possible.

Disclosure of Legally Restricted Information to a third party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safe-guard the use and disclosure of the information. The electronic exchange of Legally Restricted Information outside of the Institution must have proper approval. In addition,

- Information Security Office must be consulted to ensure appropriate security controls are employed.
- Appropriate contract language is incorporated into any agreement.

Contact the Office of Administrator for appropriate contractual language.

Storage and Protection: Legally Restricted Information in paper form must be stored in locked or otherwise secured areas when not in active use. Legally Restricted Information in electronic form must be stored in secure designated mediums or, if authorized to be stored elsewhere, only in encrypted (or similarly protected) form. It must not be stored on desktop, laptop or other portable devices or media without encryption or similar protection.

Transmission: Reports and communications should not include Legally Restricted Information unless essential to perform the function for which the communication is made. Transmission of Legally Restricted Data must be by secure methods. If Legally Restricted Data is transmitted by e-mail or other electronic transmission, it must be encrypted or otherwise adequately protected.

Destruction: When a record containing Legally Restricted Information is no longer needed, it must be disposed of in a manner that makes the Legally Restricted Data no longer readable or recoverable.

Destruction of paper records containing Legally Restricted Data normally should be accomplished by shredding. Destruction of electronic records containing Legally Restricted Data begins with deleting the data from its storage location.

Student information is protected by government laws and the Institution policies. Because of the extensive educational activities of the Institution, many people within the Institution have a legitimate need to access and transmit student records. The confidentiality of student records must be safe guarded, but the strict rules for storage and destruction of Legally Restricted Information are not always appropriate for all student records.

Reporting Unauthorized Disclosure of Legally Restricted Information: Prompt reporting of unauthorized disclosure of legally Restricted Information is essential for the Institution to meets its obligations under law, regulation, and contract. The Institution will not take disciplinary action against any person solely because of his or her good faith reporting of a disclosure. Individuals who report violations of institution policies will be protected from retaliation resulting from providing information. Individuals who report violations of policies can remain anonymous.

## II. Confidential Information

Information can be sensitive or proprietary and the Institution users may have reasons to treat it as confidential.
Examples of Confidential Information could include but are not limited to:

- Communications or records of the Governing Board and senior administrators
- Faculty research or writing before publication or during the intellectual property protection process
- Student grades
- Payroll data
- Administratively maintained employee data such as residence address information, employment history
- Performance reviews
- Alumni and donor information
- Information that the Institution has agreed to hold confidential under a contract with another party

Restriction of Information as Confidential: If a faculty or staff member is responsible for information that is sensitive, proprietary or otherwise in need of confidential treatment, the individual should clearly label the information “Confidential”. The word Confidential should be placed prominently on the information in a form appropriate to the medium in which it exists with an understanding that the purpose of the label should be to warn others clearly that this information is Confidential and should be treated accordingly.

Storage, Transmission, Access and Destruction: The rules set forth in the section dealing with Legally Restricted Information should be applied to all Confidential Information.

## III. Internal Institution use only Information (restricted)

Much information necessary for people to perform their work at the Institution is properly available to others at the Institution, but is not appropriate to be known by the general public. Information for Internal Institution use only is protected behind electronic firewalls or in private paper files in secured offices and is not accessible by the public at large. This is appropriate and will continue. Common sense and good practice dictate that this information remains accessible on a need to know basis by employees and sometimes by students, but not accessible by the media or outsiders.
Examples of Internal Information could include but are not limited to:

- Budgets
- Proposals

- Contracts/ MoUs
- Policies and procedures
- Correspondence
- Grant related documents
- Financial records
- Course materials, including on-line media
- Prospective student status information accessible to that student
- Administrative information exchanged with vendors using electronic protocols
- Student and registration information accessible online to that student
- Institution organizational charts and job descriptions.
- Reports, files or working papers concerning daily academic and administrative activities
- Travel plans of faculty or staff
- Strategic plans such as college expansion, new academic programs being considered or Departmental plans

# IV. Public Information

Public information is information that is available to all members of the Institution community and may be made available to the general public. The Institution reserves the right to control the content and format of Public information.

Examples of Public Information could include but are not limited to:

- Published marketing brochures
- Published curriculum information
- Public notices of Institution public events such as concerts and sporting events
- Schedule of classes
- Approved census facts
- Audited financial statements
- Employment opportunity bulletins
- Institution web site information

Users of college systems, both electronic and physical, are responsible for protecting the information processed, stored or transmitted using these resources, and for incorporating industry standard best practices into their daily activities.

# IV. Standard Practices

## A. Protecting Confidential Information

- DO NOT store confidential data in any college system, both electronic and physical, unless the persons who have access to that system have a legitimate need to know the information involved.
- DO NOT distribute confidential or sensitive data to external entities unless approved by the appropriate authority.
- Only distribute confidential information to internal entities on a need to know basis.
- Assume all student information is private unless the student has signed a consent form.
- Use secure means to transmit confidential data.

## B. Securing Physical Space/Data

- Physical spaces such as filing cabinets, offices and workrooms containing protected institution information shall remain locked when unsupervised.

## C. Securing Information on Workstations and other electronic systems

- Utilize strong passwords to minimize the risk of a password being compromised and data being lost due to unauthorized access. All system/network/email passwords must meet the Password Requirements policy.
- Do not share account names and passwords if the account was not configured to be a shared account.
- DO NOT open attachments and links embedded in emails unless you are confident the email is from a reliable source and intended to be sent from that source.
- DO NOT enter your username and password into an Internet form to "Verify" your credentials. Information Technology Department will never ask you to verify your username and password in that manner.
- Log out of public systems when finished working.
- Log out or lock college assigned systems when finished working.
- DO NOT save passwords in web browsers or e-mail clients when using a public computer system.
- DO NOT post college material on any publicly-accessible computer or website unless first approved by the appropriate authority.
- DO NOT intentionally damage, alter, or misuse any college-owned or maintained hardware, software, or information.
- DO NOT test security controls in place at the college or any other location (including ethical hacking) without authorization from the Information Technology Department authority.
- Secure devices by requiring a password when the device is turned on and when the screen saver is deactivated.
- All computers (desktops/laptops) accessing Institution electronic data must run up-to-date anti-virus/malware software. Exception may be made with approval from the Information Technology Department authority.
- All mobile devices (smart phones/tablets) must adhere to the Mobile Device Security policy
- Keep all computer systems up to date with the latest software maintenance releases.

## D. Communicating Security and Confidentiality Issues

- Notify the IT Department immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
- Notify the IT Department if sensitive or critical college information is lost or disclosed to unauthorized parties, if any unauthorized use of college systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.
- Forward information pertaining to security-related problems to the IT Department authority immediately. DO NOT further distribute this information.
- DO NOT discuss information security-related incidents with individuals outside of the college, or with those inside the college who do not have a need to know.

# Section IV – Specific Policies

## Acceptable Use Policy

**Purpose**
This is about Institution's Computer and Communication facilities, including those dealing with voice, data, and video. It relates to the use and administration of telecommunications equipment (including computer networks involving the PBX and Internet) as well as servers, workstation, and personal computer systems and DVRs.

**Scope**
This policy applies to any individual using or administering Institution's computer and/or communication facilities, including but not limited to both wired and wireless networks. However, what is not covered are activities solely involving personal property.

**Guidelines**
Data communication facilities at Salesian College have been provided to encourage widespread access and distribution of data and information. Computing systems facilitate manipulation and sharing of data and information. Together, these systems and facilities can be used in similar fashion to mail and telephone services, and so are governed by principles of appropriate use for those services.

Institution's communication and computing resources are used to support the educational, research, and public service missions of the institution. Activities involving these resources must be in accord with the Institution's codes of conduct, Employee handbook, student handbooks, and relevant local, state, national, and international laws and regulations. Access to computer systems and networks owned or operated by the institution imposes certain responsibilities and obligations and is granted subject to institution policies, and local, state, and national laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

***In making acceptable use of resources one must:***

- Use resources only for authorized purposes.
- Protect one's user-id and system from unauthorized use. One is responsible for all activities on his/her user id or that originate from his/her system.
- Be considerate in one's use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

***In making acceptable use of resources one must NOT:***

- Use another person's system, user-id, password, files, or data without permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to institution data.
- Use institution systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- Make, use, or distribute illegal copies of copyrighted materials or software, store such copies on institution systems, or transmit them over institution networks.

- Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or user-id.
- Waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the institution's systems or networks for personal gain; for example, by selling access to your user-id or to institution systems or networks, or by performing work for profit with institution resources in a manner not authorized by the institution.
- Engage in any other activity that does not comply with the aforementioned General Principles.

**Reporting suspected security breaches**

Anyone who has reason to suspect a deliberate or significant breach of established security policy or procedure should promptly report it to the appropriate Department Head, Dean, or Vice Principal and to the Office of Administrator. If it is felt the breach is serious and needs immediate attention, the Institution Office or local law enforcement should be contacted. The IT Department should be informed about suspected breaches and can help in any investigation.

**Information Disclaimer**

Individuals using computer systems owned by Salesian College do so subject to applicable laws and Institution policies. Salesian College disclaims any responsibility and/or warranties for information and materials residing on non-institution systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the Governing Body, the Management, its faculty, staff, or students.

# E-Mail Usage Policy

**Purpose**

Electronic mail services are provided to enhance communication among members of the College community, its alumni, and friends. Use of Institution email services must be appropriate, responsible and consistent with both the law and local standards of decency and taste.

**Scope**

All students, faculty, and staff are assigned an e-mail account in *salesiancollege.net* domain. In addition, alumni in good standing with the Institution are allowed to maintain an Institutional e-mail address for life. Members of the Management and authorised employees are entitled to have e-mail accounts in *salesiancollege.ac.in* domain (in particular if they are involved in research and publications). In the normal process, accounts will be removed when you are no longer a student or employee of the Institution.

**Responsibilities**

Members of the Salesian College community are expected to:

- Check their official e-mail on a regular basis as important course assignments and other institution information will be delivered to one's official e-mail address.
- Report any compromised e-mail passwords or any suspected breach in security.
- Make backup copies of important messages and other e-mail documents and keep those outside the e-mail system.
- Delete large files and not keep large amounts of e-mail on official e-mail servers. This means that both the number of messages and the total space devoted to storing one's messages should be kept to a reasonable level. Each user of institution e-mail is responsible to delete any unsolicited and unwanted e-mail messages (SPAM). The IT Department will assist in reducing the size of mail store upon request.

**Strictly prohibited activities**

Those using the institution e-mail system agree not to:

- Read someone else's e-mail
- Look through files that do not belong to them
- Use institution e-mail system for personal gain or commercial reasons.
- Allow someone else to use their e-mail account or password
- Use another person's e-mail account to send or read mail
- Cause a name other than their own to appear in the From: or Reply-To: section.
- Consume network resources by sending large attachments
- Send an e-mail containing the same content to large numbers of people.

# Password Policy

**Purpose**

IT infrastructure in use in the Institution consist of Computers (Desktops / Laptops/ Tabs), the ERP System, LMS System, Library Management System (eBLIS), Accounting System, DVRs, ORELL (Spoken Language) System and Networks. Use of these systems must be appropriate, responsible and consistent with both the law and institution policies.

**Scope**

All faculty and staff who are assigned personal computers or laptops need to have password protected systems. Students who use laboratory computers also login to password protected machines. Moreover, the ERP system, LMS system and Library Management system have separate logins, and each student and faculty have been provided with separate user-ids for these systems. Other than these, Institution also provides wireless connections for the internet access.

**Password Requirements**

Maximum password age
a. Faculty = 180 Days
b. Staff = 90 Days
c. Students = 365 Days

2. Minimum password length = 8 characters
3. Password must contain 3 of 4 of the following items
    a. Capital Letter (ABC…..)
    b. Lowercase letter (abc….)
    c. Number (123)
    d. Special Character (?!|….)
4. Passwords cannot contain common dictionary words
5. Passwords cannot contain keyboard patters (qwerty)
6. Maximum times a character can be repeated = 2 (aa…33)
7. Cannot reuse last 3 passwords
8. Passwords cannot contain user's display name
9. Passwords cannot contain user's user name

# Inappropriate Material Policy

**Purpose**
As a Don Bosco institution, Salesian College maintains high moral and ethical standards.

**Scope**
Members of Management, faculty, staff, students, IGNOU faculty and students.

**Responsibilities**
If you are the recipient of inappropriate material, or end up at an in appropriate website, it is important that you:

- Delete this material or close the web browser immediately;
- You must also advise your manager or a staff member that you have received or accessed such content. If the sender is known to you ask them to stop sending inappropriate material to institution email accounts.

Users must not access, create, download, print, store, forward or send inappropriate content. Examples of which include, but are not limited to:

- Information or images containing indecent material (this includes pornographic or other sexually explicit material), or other material, which explicitly or implicitly refers to sexual conduct or preference.
- Information or images containing profane of abusive language. This includes anything that refers to or supports discrimination of any kind.
- Unwelcome propositions.
- Any defamatory, illegal, offensive, annoying or harassing material.
- Information intended to incite criminal activities or instructs others how to commit such acts.

If one is in doubt as to whether the material he/she is accessing is inappropriate, it should be treated as such and remove it from one's computer.

All official communications between faculty and students shall be between 6:00 am and 8:00 pm. Among faculty or colleagues in the department it shall be from 5:00 am to 10:00 pm. In case of emergency discretion is to be maintained that does not encroach on the privacy and personal time of the other.

# Biometric Information Privacy Policy

## Statement

Salesian College uses biometric identification systems to increase security and control access to certain campus facilities. The Institution recognizes the sensitivity of Biometric Information and takes seriously its obligations to maintain the confidentiality and protect the security of data.

### Purpose

In accordance with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, this policy sets forth the Institution's procedures for disclosure, storage and destruction of Biometric Information.

### Scope

Faculty, staff, students and third party contractors.

### Definitions

*Biometric Identifier*. A fingerprint, voiceprint, retina or iris scan, hand or face geometry scan.
*Biometric Information or Biometric Data*. Information based on a person's biometric identifier that is used to identify that person.

## Policy Implementation

*I. Consent*

An individual's Biometric Data will not be collected or otherwise obtained by Salesian College without prior written consent of the individual. The consent form will inform the individual of the reason the Biometric Information is being collected and the length of time the data will be stored.

*II. Disclosure*

The Institution will not disclose or disseminate any Biometric Data to anyone other than its Biometric Identifier collector vendor(s) and/or licensor(s), unless:
a. Disclosure is required by state or national law or municipal ordinance; or other identifier;
b. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction,
c. The disclosed data completes a financial transaction requested or authorized by the employee; or
d. The employee has consented to such disclosure or dissemination.

*III. Storage*

In circumstances where Salesian College retains Biometric Information, the institution will use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic Biometric Data collected. Storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the institution stores, transmits and protects from disclosure other confidential and sensitive information that is used to uniquely identify an individual.

*IV. Retention Schedule*

In circumstances where institution retains Biometric Information, the institution will permanently destroy an individual's Biometric Data within six (6) months of when the initial purpose for collecting or obtaining such Biometric Data has been satisfied, such as:

a. The employee's employment is terminated;
b. The student graduates or otherwise leaves the institution;
c. The employee transfers to a position for which the Biometric Data is not used; or
d. The institution no longer uses the Biometric Information.

If any institution's vendors and/or licensors require access to Biometric Data in order to fulfil the purpose of collecting such information, the institution will request that they follow the above destruction schedule.

The recording of the closed circuit TV in operation in the campus(es) shall be retained for the said duration, such systems are auto designed and in case of need for the duration of the requisite legal/ scrutiny purposes.

# Social Media Usage Policy

**Statement**
This policy provides guidance for use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

**Scope**
Faculty, staff, students, alumni, industry collaboration partners, IGNOU faculty and students.

**Responsibilities**
The following principles apply to professional use of social media on behalf of Salesian College as well as personal use of social media when referencing the Institution.

- One needs to know and adhere to the Code of Conduct when using social media in reference to the institution.
- One should be aware of the effect his/her actions may have on his/her images, as well as the institution's image. The information that one posts or publishes may be public information for a long time.
- One should be aware that the institution may observe content and information made available by him/her through social media. One should use his/her best judgment in posting material that is neither inappropriate nor harmful to the institution or its stakeholders.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.
- One is not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, one should check with the Office of Administrator and/or supervisor.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. One should refer these inquiries to authorized Institution spokespersons.
- If one encounters a situation while using social media that threatens to become antagonistic, one should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- One should get appropriate permission before referring to or posting images of current or former employees, students, vendors or suppliers. Additionally, one should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with one's responsibilities at the institution. Institution's computer systems are to be used for business purposes only. When using institution's computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Instagram, Institution blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Subject to applicable law, after-hours online activity that violates the Institution's Code of Conduct or any other institution policy may subject a person to disciplinary action or termination.
- If one publishes content after-hours that involves work or subjects associated with the institution, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent institution's positions, strategies or opinions."
- It is highly recommended that one keeps institution related social media accounts separate from personal accounts.

# Mobile Device Security Policy

**Purpose**

This policy defines standards, procedures, and restrictions for any and all end users with legitimate business uses connecting mobile devices to Salesian College's networks, digital resources, and data. The mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- Portable gaming devices
- Laptop/notebook/ultrabook computers
- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

In order to enforce security and remote device management, only devices that meet the following criteria are allowed to access Institutional resources:

- Smartphones, tablets, and other devices running Android version 2.3 (Gingerbread) and higher.
- Smartphones and tablets running iOS 5.0 and higher.
- Laptops running Windows 7 and higher
- Laptops running Mac OS X Cheetah (10.0) and higher

The policy applies to any mobile device that is used to access institutional resources, whether the device is owned by the user or by the organization.

**Scope**

This policy applies to all institution employees, including full and part-time staff, contractors, freelancers, and students who use any mobile device to access, store, backup, or relocate any organization or client-specific data.

**Security**

1. Employees/ students using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password[cfr section on password in this policy]; a PIN is not sufficient. All data stored on the device must be encrypted using strong encryption. See password policy for additional background. Employees/ students agree never to disclose their passwords to anyone.
2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.
3. Any non-institution computers used to synchronize or backup data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by the institution's IT department.
4. Passwords and other confidential data, as defined by Institution's IT department, are not to be stored unencrypted on mobile devices.
5. Any mobile device that is being used to store or access institution data must adhere to the authentication requirements of institution's IT department. In addition, all hardware security

configurations must be pre-approved by institution's IT department before any enterprise data-carrying device can be connected to the institution network.

6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with institution's security policy.
7. Employees/ students, contractors, and temporary staff accessing institution internet resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing institution resources of any kind.
8. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase institution-specific data from such devices once its use is no longer required.
9. Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.
10. Unauthorized usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.
11. Applications that are not approved by IT are not to be used within the workplace or in conjunction with institution data.

# Section V – Enforcement

Violations of this Policy will be handled under normal disciplinary procedures applicable to the relevant persons or Departments. The Institution may suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Institution resources or to protect the Institution from liability. The Institution routinely monitors the use of Information Technology Resources to assure the integrity and security of Institution resources. The Institution may refer suspected violations of applicable law to appropriate law enforcement agencies. Violations of this Policy can result in disciplinary action up to and including separation from the Institution and/or exclusion from Institution programs, facilities and privileges. Violations of law can lead to fines, injunctions and personal liability.

The university considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on university systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violators are subject to disciplinary action as prescribed in the Institution's Personnel Policies, employee and student handbooks.

Offenders also may be prosecuted under government laws (please refer to the Reference section)

# Section VI – Approval and Review

This Information Technology Policy Handbook has been compiled by the Tech Team of Salesian College. It has gone through due process of peer and management review and approval.

Proper and responsible use of Institution IT Resources need continual process improvement and need further Policy and procedural development from time to time. Future revisions will likely include additional materials and the institution reserves the right to change the policies if need arises.

Approved By,

(Head, Tech Team)

Authorized By,

Fr. George Thadathil,
Principal, Salesian College

# Section VII – References

References:

- Information Technology Act, 2000 ('the IT Act')
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules');
- National Cyber Security Policy 2013
- Personal Data Protection Bill, 2019 ('the Bill');
- Non-Personal Data Governance Framework ('the NPD Framework'), which is currently being deliberated by the Committee of Experts constituted under the Ministry of Electronics and Information ('MeitY'), whose reports on non-personal data can be accessed here and here;
- India - Data Protection Overview