



ICT Email Policy

Revision History

Version:	1.0
Version update history:	Initial Release
Effective date:	01-07-2024
Prepared by:	Immanuel Wonderful C J
Approved by:	Suresh Gurala

Contents

Revision History	2
Contents	3
1. Purpose	4
2. Scope	4
3. Objectives	4
4. E-Mail Format	4
5. E-Mail groups	5
6. Monitoring	5
7. Policy Statement	5
8. Data Retention	6
9. Enforcement	7

1. Purpose

The purpose of this email policy is to ensure the proper use of Sreenidhi's email system and make users aware of what Sreenidhi deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Sreenidhi's Network.

2. Scope

This e-mail policy provides guidelines regarding the following aspects of e-mail as an official means of communication:

- Official use of e-mail for staff
- Student use of and responsibilities associated with assigned e-mail addresses
- Expectations of e-mail communication between faculty and student and staff and student
- Storing documents on Google drive and sharing internally

3. Objectives

The principal of this policy is to describe the acceptable use of the Sreenidhi's email and related services, systems and facilities.

The objective is to build a long-lasting relationship with Students, Staff, and Interested Parties based on a foundation of trust. It is policy that all personal information collected, including that of customers, donors, sponsors, volunteers and staff of Sreenidhi, is kept in the strictest confidence by Sreenidhi and will not be disclosed and/or sold or traded to anyone except Sreenidhi's staff, students and management.

4. E-Mail Format

E-mail IDs will be created using the following format:

- Staff
 - {FirstName}. {First letter of Initial}@suh.edu.in. For example, for a staff member named Halavath Surya, the email ID will be surya.h@suh.edu.in and the display name will be visible as Surya H .
 - For staff members in key positions, where past mail correspondence is required, or who has extensive external communication or for admin staff, the designation-based email IDs will be created (e.g. Principal, Director, Accounts Manager, Manager Facilities, etc).
 - The email IDs of departing Sreenidhi staff will be suspended on their last working day. The email IDs will be kept for 90 days and then they will be permanently deleted. For

designation based email ID's password will be reset and assigned to new member taking over the role.

- Student
 - RollNumber@cse.sreenidhi.edu.in. The display name will include the student's roll number, name, and section. For example, 23311A1101 (A) Ramesh will be displayed.
 - The email addresses of students who passed out in the last two years will be kept for placement purposes only for two years and then they will be permanently deleted.

5. E-Mail Groups

E-Mail groups created and the ownership will be given to the group owners who are responsible for the addition and deletion of the group members. Additionally, ICT will initially assign the users to default department groups based on Teaching and Non-Teaching.

ICT will create additional groups based on requests received from Heads of Departments

6. E-mail Create and Update

Receive request from HR and Registrars office with following information

- Staff
 - First and Last Name
 - Department
 - Designation
 - Mobile
 - Personal e-mail id
 - SAPID
 - Teaching / Non-Teaching
 - Email ID to be mentioned in case it is designation based
- Student
 - First and Last Name
 - Department
 - Section
 - Mobile
 - Personal e-mail id
 - Roll No

Create email and assign to requested groups. Updates on change of above fields will be handled on request from HR.

7. Monitoring

While we respect the privacy of employees, IT department under management guidance had deserved the right to review, audit, intercept, access and disclose communications created sent received or stored using E-mail system, with or without prior notice for the following purposes, but not limited to

- Preventing unauthorized access and system misuse
- Security incident investigation for violation of security policies
- Compliance with legal and regulatory requirements
- Staff are provisioned with 15GB Google drive space while Students have 10GB. Any exceptions will need approvals from HoD.

8. Policy Statement

- Use of email must be consistent with Sreenidhi's policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Sreenidhi's email account should be used primarily for Sreenidhi's business- and Work- related purposes; personal communication and non-Sreenidhi related commercial uses are prohibited.
- Students are expected to use their Sreenidhi's email address when communicating electronically with the Sreenidhi Staff, including communicating with faculty. Email messages received from students using Sreenidhi's email system will be treated as legitimate.
- Sreenidhi's data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- The Sreenidhi's email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Staff who receive any emails with this content from any of Sreenidhi's staff, students should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding Sreenidhi's email to a third- party email system. Individual messages which are forwarded by the user must not contain Sreenidhi's confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Sreenidhi's business, to create or memorialize any binding transactions, or to store or retain email on behalf of Sreenidhi. Such communications and transactions should be conducted through proper channels using Sreenidhi's approved documentation.

- Sreenidhi's Student, Staff, Faculties shall have no expectation of privacy in anything they store, send or receive on Sreenidhi's email system
- Sreenidhi may monitor messages without prior notice.
- Users must not forward chain letters, junk mail, jokes and executables
- Users must consider the size of attachments and keep them as small as possible
- Create and use an email signature. Members of staff should use signatures which include their name, job title, phone number and 'address of Sreenidhi'.
- Only mark emails as 'high priority', 'urgent' or 'important' if they genuinely are; the impact of using these markings will be reduced if they are used too often and inappropriately.
- When sending emails to a group of recipients, consider whether the 'Bcc' facility is more appropriate than the 'To' or 'Cc' facility. This could be the case where you are emailing a group who do not know each other, and you need to ensure they can't see each other's email addresses or where it is not appropriate for each recipient to know who else has received the email.
- Staff should check their email at least once each working day. If this is not possible, an appropriate 'out of office' reply should be turned on, stating when the account will be checked and who can be contacted in the meantime if the email needs urgent attention.
- Students should check their Sreenidhi's email accounts frequently.
- Email received from an unknown sender/third party kindly do not click on any link or do not open any attachments of that mail.

9. Data Retention

- Information Held
 - These documents are updated at least once a year as will testify the revision history. The owner of these documents is the Chief Technology Officer
- Information Collected
 - Sreenidhi may collect, store and use the following kinds of personal dataInformation about your computer/Mobile and about your visits to and use of our services including our website and end-user facing technology.
 - Information relating to any transactions carried out for us to fulfil requests in association with our defined scope of work.
 - Information that you provide to us to register your personal profile and for access to our technology.
 - Any other information that you choose to send to us which is pertinent to the scope of work.

10. Enforcement

Any Staff/Student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.