	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

INFORMATION TECHNOLOGY (IT) USAGE POLICY OF JAWAHARLAL INSTITUTE OF POSTGRADUATE MEDICAL EDUCATION AND RESEARCH (JIPMER), PUDUCHERRY



Drafted by	Checked by	Verified by	Approved By
Deputy Officer In-charge, Hospital Information System (HIS), IT Wing, JIPMER	Head of IT Wing JIPMER	Law Officer, Legal Cell, JIPMER	Director JIPMER



	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

TABLE OF CONTENTS

Sr. No.	SECTION	Page No.
1	Introduction	1
2	Scope	1
3	Objective	1
4	Roles and Responsibilities	1
5	Access to the Network	2
	5.1 Access to Internet and Intranet	2
	5.2 Access to Government Wireless Networks	3
	5.3 Filtering and blocking of sites	3
6	Monitoring and Privacy	3
7	E-mail Access from the Government Network	4
8	Access to Social Media Sites from Government Network	4
9	Use of IT Devices Issued by Government of India	5
10	Responsibility of User Organizations	5
11	Security Incident Management Process	6
12	Scrutiny/Release of logs	6
13	Enforcement	7
14	Deactivation	7
15	Review	7
16	Glossary	8

	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

1. Introduction

JIPMER provides IT resources to its faculty, staff, residents, and students to enhance knowledge, efficiency, and productivity. These resources include desktops, laptops, mobile devices, printers, scanners, networks (including wireless), Internet connectivity, and software. Misuse of these resources can expose the institute to risks and liabilities. Therefore, their usage must be lawful, ethical, and primarily for official purposes.

2. Scope


This policy applies to all employees, residents, students, researchers, and staff of JIPMER, including visiting faculty and deputed personnel, who use the IT resources of the institute.

3. Objective

The objective of this policy is to ensure proper, secure, and efficient access to JIPMER's IT resources, prevent misuse, and maintain compliance with institute norms and the IT Act 2000.

4. Roles and Responsibilities

- Competent Authority: Director, JIPMER
- Designated Nodal Officer: Faculty In-charge, IT Wing, JIPMER
- Implementing Agency: IT Wing of JIPMER (with support from NIC for network services)
- Nodal Agency: IT Wing of JIPMER

	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

5. Access to the Network

5.1 Access to Internet and Intranet

- Users must register their systems and obtain approval before connecting to JIPMER's network.
- Sensitive departments must maintain separate Internet and Intranet systems.
- Unauthorized attempts to bypass firewalls, filters, or VPN restrictions are prohibited.

5.2 Access to Institute's Wireless Networks

- Devices must be registered and approved by the IT Wing before connecting to JIPMER's wireless networks.
- Authentication is mandatory for access.
- Users must avoid connecting institute devices to unsecured external wireless networks.

5.3 Filtering and Blocking of Sites


- The IT Wing may block content that violates Indian law, institute policy, or poses a security/productivity risk.

6 Monitoring and Privacy:

The IT Wing has the right to audit systems and networks for compliance. For legal or security reasons, the IT Wing may access, review, copy, or delete electronic files, emails, or Internet logs, with intimation to the user.

7 E-mail Access from the Government Network

- Official email must only be through institute-authorized services.
- Private email servers must not be accessed through the JIPMER network.
- Personal correspondence may be done using name-based JIPMER email IDs.

	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

8 Access to Social Media Sites from Government Network

- Use must comply with Government of India’s “Framework and Guidelines for Use of Social Media by Government Organizations.”
- Confidential, defamatory, offensive, or unlawful content must not be posted.
- Objectionable incidents should be reported to the IT Wing immediately.
- Users must use high-security settings on social networking sites.

9 Use of IT Devices Issued by institute

- IT devices must be used primarily for official purposes and in compliance with institute and Gol guidelines.
- Best practices for desktops, laptops, mobile devices, external storage, and peripherals must be followed.

10 Responsibility of Institute

Policy Compliance:


- The IT Wing will implement controls to ensure compliance.
- Regular reporting mechanisms and awareness programs will be conducted.
- Unauthorized installation of network/security devices is prohibited.

Policy Dissemination:

- The policy must be circulated widely.
- Orientation programs for new staff must include awareness about this policy.

11 Security Incident Management Process

- Any incident that compromises confidentiality, integrity, or availability of data must be reported immediately to the IT Wing.
- The IT Wing may deactivate/remove devices if deemed a threat, under intimation to the Director.

	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

12 Scrutiny/Release of logs

- Logs will be released only to law enforcement agencies as per IT Act 2000.
- Requests from other organizations will not be entertained without due legal process.

13 Enforcement

- This policy is mandatory for all users of JIPMER's IT resources.
- Departments are responsible for compliance within their units, with support from the IT Wing.

14 Intellectual Property


- Users must not use JIPMER's IT resources in a way that infringes on intellectual property rights, including copyrights, patents, and trademarks.

15 Deactivation

- The IT Wing may deactivate/remove any device posing a security risk.
- Affected users and the Director will be informed accordingly.

16 Review

- This policy will be periodically reviewed and updated by the IT Wing with approval from the Director.

	Title of Document	Version	Date of Issue
	IT Usage Policy of JIPMER Puducherry	1.1	08-09-2025

17 GLOSSARY

- End User: All employees, residents, students, and staff of JIPMER.
- Competent Authority: Director, JIPMER.
- Nodal Officer: Head of IT Wing, JIPMER.
- Implementing Agency: JIPMER IT Wing.
- Intranet: A private internal network of the institute, separate from the Internet.
- Endpoint Compliance: Security approach requiring devices to meet standards before accessing the network.
- Wireless: Institute wireless networks, to be deployed securely.
- Social Media: Includes blogs, forums, networking sites, newsletters, and related services.
- Security Incident: Any event that compromises confidentiality, integrity, or availability of institute data.