Inderprastha
Dental College & Hospital

IT POLICY

The IT policy of the Inderprastha Dental College and Hospital covers the following points:-

1. SERVER MANAGEMENT

The internal server deployed in the premises of the institute is looked after by the IT team IPDC. Operating system configuration should be in accordance with the current requirement of the institute. The server access records should be monitored on regular basis by the authorized personnel.

2. SERVER ROOM ACCESS

Only authorized person or staff should be allowed in the server room. Entry into the server room by tailgating other staff is not allowed. No eatables are allowed in the server room. The people who violate these rules are liable to be penalized for trespassing/breach of protocol as per the institution's policy.

3. SERVER HARDENING

The server hardening policy should describe the requirements for installing a new server and maintaining the security integrity of the server and application software.
The server must be connected to IPDC Network. Operating system should be approved from an IT approved source. Unnecessary software and drives should be removed.
Violation of this policy may be subjected to disciplinary action.

4. NEW PASSWORD

This policy facilitates the confidentiality, integrity and availability of data across the infrastructure. Passwords are the entry points to the IT Resources, since the access to the resources is important in maintaining the security of the system.
Passwords for institutional email IDs and system log in should not be less than 8 characters, including a mix of alphabets, numbers and special characters. Passwords should be changed at regular intervals. Passwords should not be shared or revealed to anyone, besides authorized users. Unauthorized sharing of passwords should be considered as a serious breach of the IT security.

5. USER CREATION AND WORKSTATION SECURITY

Each computer system whenever added to infrastructure should be accessed only through a proper computer – name or user – ID and password generated by the IT team. If there is a need to change the user ID, it should be done after approval from the concerned authority.
Also under the work station security policy, local administrator password should be created on all the workstation in the institute and should be kept with the IT team.
Access to the confidential files should be password protected with a strong password.

6. E- MAIL ID CREATION

Institutional email accounts should be created using the standard format provided by the admission department

Students accounts should be created based on the data provided from the admission department.

The e- mail privileges should be terminated for the staff or students upon leaving the institute.

7 .WI – FI USAGE

The IPDC Campus is wi-fi – enabled and this services are availed free by students and the Staff.

8. ANTI – VIRUS

IT team should ensure that each system i.e., PC, laptop etc in the institute should contain an authorised/standard antivirus software installed. It should be regularly updated to protect the institute network and systems from virus attack. To prevent the transmission of spam or non – business related contents, antivirus software is must.

9. SYSTEM AUDIT

The members of the IT department of IPDC are authorised to conduct a security audit on any system in the institute to ensure the integrity, confidentiality and availability of information resources.

The audit may be performed through user level or system level access to any computing or communicating devices.

10. NETWORK CABLING

It should be done and maintained by qualified engineers to ensure the integrity of the cable and wall mounted sockets.

Any unusual network wall sockets should be sealed off.

11. IT HELP DESK

The maintenance of all the system in the institute is managed by the IT Team. There should be AMC for the expensive parts. Whenever there is any problem with the software/ hardware/link; it should be informed to the IT team.

If the person needs the involvement of a third-party service provider, it should be reported to authorised personnel through proper channel. Regular follow up should be done with the service provider.

After the problem gets resolved, the functioning should be observed for a specific time (7 working days) before closing the complaint.

12. MEDIA HANDLING

There should be a proper disposal of the electronic media containing sensitive data. All the media should be handled only by the person nominated to do so.

For disposal of the old condemned systems, the e – waste disposal policy of the institute should be followed.

13. BLOCKAGE OF ACCESS TO CERTAIN SITES

The internet access to the system should only be with the academic or administrative purpose. The access to social media sites should be blocked for the users.

The institutional IT policy will be subjected to review annually or as and when required.