

Annexure – I

Joining Checklist

I _____ (Name, Designation & Department of the Employee) declare that I will:

Physical Access

- use an authorized pass/ ID card for entry to AIIMS Raipur premises.
- use the biometric and facial recognition system to access the premises.
- take prior approval if asked to stay in the premises after working hours.
- take prior approval if asked to report on a leave day.
- adhere to work timings prescribed by the AIIMS Raipur.
- only attend virtual meetings using approved platforms for related work due to the sensitive nature of data.
- not allow any unauthorized personnel to enter the premises.

Hardware Access

- access data only on the allotted device using login credentials and Virtual Private Network (VPN),
- use only authorized Wi-Fi connection provided by AIIMS Raipur,
- do not carry any personal external Wi-Fi devices/network equipment such as dongles for accessing the internet,
- do not use my personal mobile phone/I-pad to access,

Data Management Guidelines

1. Data Access

- access the portal through authorized devices and credentials only,
- render duties as per the role provided,
- access the data based on role and policies,
- accept data only shared through proper channels i.e., approved by the AIIMS Raipur competent authority.

2. Data Handling

- use data only for the purpose defined by the AIIMS Raipur,
- don't access illegal/blocked Websites, portals, applications, open databases in AIIMS Raipur network.

3. Data Transfer

- transfer data as per the AIIMS Raipur guidelines only,
- take Prior approval if hardcopies need to be carried outside the AIIMS Raipur premises,
- use the official printer provided to print only AIIMS Raipur documents,
- not use any social media platform to circulate data generated in AIIMS Raipur,
- not use any unauthorized electronic gadgets (hard disks, pen drives, Bluetooth devices) for the transfer of data or information,
- not publish the data in any external report/document,

4. Data Storage

- store data on an authorized cloud storage,
- not store data on any external cloud/external devices,

Social Media

- not click any picture or video,
- not use credentials for personal use on any social media platform,
- not post any confidential data on any social media platform,
- not express any personal views on social media platforms pertaining to the data,
- not circulate any data or information on any social media platform,

I have read and will adhere to all the above points and guidelines.

Name:

Signature:

Date: