IT Policy

Updated May, 2023

1. Information Ownership

- All Organization data as defined in the below section of this policy is owned by the Doctors For You (DFY).

2. Definitions

- **Organizational data-** includes files (paper and electronic), pictures, videos, creative work of art, email messages, voice messages, and faxes regarding activities of/in DFY.
- **Personal Data** – Files that an employee would expect to take with them should be secured.

3. General Use

- Computer, Internet, and email use are subject to all other Doctors For You Department policies, including but not limited to those concerning harassment.
- The display or transmission of inappropriate images and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-colour jokes, or anything that may be construed as harassment or showing disrespect for others. Employees are expressly forbidden to access Internet sites where potentially offensive material is located. Downloading or viewing pornography or other questionable material is not allowed and may be subject to review and subsequent disciplinary action.

4. Personal Use

- Email, Internet access, and computers in DFY resources/ premises should be used primarily for Organization purposes.
- Employees are permitted to use computers, non-organisational email accounts, and the Internet for personal use provided such use is limited in quantity, and is done on the employee's time and gives all information only about the personal affairs.
- Personal use of the Internet while connected to official networks is expressly prohibited until the official end time.
- Streaming or downloading music or movies is prohibited. Personal data may reside only on organization computers C drives.
- Personal use of computers is subject to the following:
  - Employees' email accounts, Internet access, and computer use may be monitored and reported on by the IT Dept.
  - Employees should not view or distribute any obscene, disparaging, derogatory, or another type of material that violates the Doctors For You's professional ethical standards.
  - Employees should not use their official email address or computer to subscribe to any email distribution lists for non-business purposes.

- Following personal data may never reside on the Doctors For You network or email system.
  - Passwords
  - Mobile Device access passcode must be maintained at all times on tablets and smartphones.
- Passwords must never be revealed to anyone for any reason other than Doctors For You IT support staff, following propose channel ie- documentation through email.
- All passwords must be immediately changed if they are suspected of being disclosed to anyone other than the authorised user.

Telecommunications and Internet

Telephone equipment, e-mail addresses, intranet and internet are provided by DFY primarily for work-related assignments. They are a tool and an organisational resource. They can be used within the applicable legal regulations and internal DFY communication policies.

There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by DFY that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of policies and/or procedures of DFY. The evaluations can be conducted only by investigating departments

while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the DFY regulations.

Internet Access

- Access to sites deemed inappropriate by management is strictly prohibited (Obscene or offensive, Illegal, Gaming, Streaming audio and video including radio stations).
- Doctors For You issued internet access is never to be used for audio or video streaming or downloading.
- Staff members are expected to limit their use of the Internet to access information that is acceptable in the workplace. This policy applies at any hour of the day, whether there are others in the building or not. Employees should remember that our systems maintain records of Internet traffic – sites that have been accessed, who accessed them, and the time of day. Staff may access the Internet for personal use during non–working hours; however, staff should use their best professional judgment in determining if such use is wise while guests or visitors are in the office.

Specific Policies & Privacy

- Employees should not allow anyone else to access any Department resources.
- Employees should never access any Department resources from any computer or mobile device not owned by the employee or the firm.
- Special care should be exercised when an employee-owned computer or mobile device is shared in a family or social setting.
- A current copy of Anti-Virus software must be installed and active on any employee-owned computer which is used for secure data.
- Employees have no right to privacy of any material created, received, or sent via email, fax, use of the Internet, or by any other computer or mobile device use.
- The organization reserves the right to monitor, log, and review, all email, Internet access, and other computer and mobile device use.
- Please be aware that deleting a file or email message will most likely not destroy it completely.
- Doctors For You has the ability and reserves the right to access all computers and email accounts without regard for any passwords.

Physical Security

- Computer and peripheral equipment other than laptops, projectors, and authorized accessories may not be removed from the Doctors For You offices.
- When driving with laptops and accessories, they must be kept in the appropriate vehicle at all times. Before taking the IT tools and laptops to the field should be counted and checked, leaving the destination the tools and laptops should be check once again for confirmation purposes.
- Laptops should never be left in cars overnight.
- If a laptop is lost, misplaced, or stolen, the Doctors For You IT department should be notified immediately.
- No one other than a Doctors For You employee is permitted to operate a company computer except with the permission of the Doctors For You IT department.
- If an employee-owned mobile device with an official email is lost, the Doctors For You IT department must be notified immediately.

Software

- The Doctors For You IT Department must approve all applications before such applications are installed.