T.M.A.E Society's
M.M.J.G. College of Pharmacy,
Ijari Lakamapur P B Road
Haveri – 581110

Security Measures

Below are 7 key measures which educational institutions will need to implement in order ensure that they are compliant with the DPA:

- **Appoint a Data Protection Officer ⟶ Dr. B M Vrushabendra Swamy**

A DPO will be responsible and account for all data protection issues within the institution. They should be referred to in the institution's data protection policy, as they will be required to deal with security-related enquires from staff members. The DPO is also responsible for training staff, investigating suspicious activity, and keeping up-to-speed with industry practices.

- **Training, Policies and Procedures**

It's very Important staff members a sufficiently trained to company with the DPA, as failure to do so could be costly, each staff member should have a clear understanding about data protection issues, and the Measures that should be taken to mitigate the risks of a potential breach. Staff members should attend at least one training course per year, which should outline the compliance protocols of the institution. Staff members should also be may aware that they may be personally liable for any breaches of the DPA. Staff members must have access to an up –to–date protection policy, which they can use as a reference if they are un sure about the correct protocol in a given scenario.

- **Working from home and BYOD**

BYOD (Bring your own device) is an increasingly popular trend, whereby organisations allow their staff members to use their own devices, such as laptops, tablets or mobile phones, in the workplace. However, there are a number of security risks associated with this movement, as institutions have less control over how these devices are managed. In such an environment, it is a good idea to use secure remote access software as opposed to allowing staff members to access their own personal email accounts and cloud facilities. Likewise, installing device management software of any devices used for accessing the institution's data, will help minimize the risk of a security breach.

- **Marketing, privacy and Consent**

Should an institution choose to use personal information, such as students' email addresses as tool for their marketing campaigns and promotions, it is important that they have consent from their subject before doing so. Likewise, if an institution were to purchase data, such as mailing lists, they must ensure that the subject involved have been informed about how their personnel information will be used, and have given their consent. Obtaining such authorization is usually done via a 'Privacy Notice', which the data subject should read and agree to.

(P.T.O)

- **Subject access request's (SAR's)**

Under the data protection Act, data subjects have the right to request any personnel information that is held by any organization or institution. It's important to note that SAR's may also include private emails, which may contain delicate personnel information.

- **Cyber insurance**

It is important that an institution's insurance policy is setup to cover potential data breaches, as the fines associated with such breaches can be very high. Insurance companies now offer cyber insurance, which is designed to cover cyber – attacks and data theft.

- **Audit! Audit! Audit!**

The need for a suite of sophisticated auditing tools is perhaps the most over looked measure of ensuring the security of your sensitive data. It is crucial that you have a past and efficient means of finding out where your sensitive data is located, who has access to what data, and when that data is accessed. You will also need a swift and intuitive means of reporting changes to the files and folders on your system.