Personal Devices Policy

Purpose

Mobile devices, such as smartphones, tablets and laptops, are important tools for the organisation and their use is supported to help achieve business objectives. However, mobile devices (whether personal or belonging to the Institute) also pose a significant risk to the Institute's information security and data protection. If appropriate security policies and procedures are not implemented, mobile devices can act as a conduit for unauthorised access to the organisation's information and IT infrastructure. This can lead to costly data breaches and system infections.

This policy aims to protect the Institute's information assets in order to safeguard its information, clients, patients/examinees, intellectual property and reputation. This document outlines a set of practices and requirements for the secure use of all mobile devices when accessing the Institute's network and aims to protect the security and integrity of the Institute's information and information infrastructure. The Institute reserves the right to restrict the use of mobile devices if users do not comply with the policies and procedures described below.

Scope

This policy applies to all mobile devices (smartphones and computers), whether owned by the Institute or by employees, which have access to the Institute's networks, information and systems, with the exception of laptops managed by the IT Manager. Limited exceptions to the policy may be made where necessary. However, a risk assessment must be carried out by the Information Security Officer and prior written approval must be granted by the Management.

Acceptable Use

- The Institute defines acceptable use as activities that directly or indirectly support the Institute's operations.
- Access to illegal/prohibited websites is prohibited during working hours or whilst employees are connected to the Institute's network. Such websites include, but are not limited to:
    - Websites containing pornographic content,
    - Child pornography websites,
    - Gambling websites, etc.
- Location data is disabled unless the employee has enabled it themselves.

- Mobile devices must not be used for:
    - Storing or transmitting illegal material
    - Storing or transmitting proprietary information belonging to another organisation
    - Harassing third parties
    - Participating in activities outside the Institute
- It is prohibited to install applications that do not originate from iTunes or Google Play.

Information Security

- To prevent unauthorised access, mobile devices must be password-protected using the device's built-in features.
- The password is strictly personal and should not be known to anyone outside the device owner's professional, family or social circle.
- Passwords must contain a minimum number of characters and be changed in accordance with the Password Policy. The password must not be the same as other credentials used within the organisation. Employees are responsible for regularly changing passwords on their mobile devices. It is recommended that passwords be changed at least every 2 months and certainly in the event that there is a suspicion that they have been disclosed to another person.

Personal data protection (compliance with GDPR & ISO 27701)

In accordance with the GDPR and ISO 27701, personal data processed by INEB in the course of its operations and research activities must not be stored on personal devices. If the processing or storage of personal data on a personal device is necessary, explicit written permission must be obtained from the Institute. Furthermore, the data retention period must be documented and appropriate technical and organisational measures (such as encryption, access control and secure deletion mechanisms) to ensure the confidentiality, integrity and availability of personal data. All users must comply with personal data protection policies to mitigate risks associated with unauthorised access, data leakage or non-compliance with regulatory requirements.

Risks / Obligations / Disclaimer

- Lost or stolen mobile devices must be reported to the Information Security Officer. Employees are responsible for notifying their mobile phone provider of the loss of a personal mobile device.

- If an employee suspects that unauthorised access has been gained to the Institute's data via a mobile device, they must report the incident immediately to the Information Security Officer.
- Employees are expected to use their mobile devices in an ethical manner at all times and to comply with the Institute's acceptable use policy as described above.

Declaration of Acceptance of the Personal Devices Policy

I have read and understood the Personal Device Policy and agree to comply with the policies and procedures set out therein. I understand that it is my responsibility to back up any information stored on the device.

Employee's full name

Signature

Date