**TECHNOLOGY POLICIES**

**SECTION 1: TECHNOLOGY**

**POLICY 3: BRING YOUR OWN DEVICE (BYOD)**

|  |  |
| --- | --- |
| **Policy Rationale** | At [organisation] we acknowledge the importance of mobile technologies in improving organisation communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to [organisation's] network and equipment. This policy sets expectations, obligations and acceptable use practices for using personal devices at or for work activities.  |
| **Policy**  | Mobile devices approved for [organization] useThe following personally owned mobile devices are approved to be used for organisation purposes:* [insert type of approved mobile devices such as notebooks, smart phones, tablets, iPhone, removable media etc.]
* Staff may use additional device models explicitly approved in writing by their line manager, providing it adheres to the guidelines in this policy

Registration of personal mobile devices for [organisation] useAny personal devices accessing [organisation] resources or information must be registered.When using personal devices for [organisation] duties, staff use will register the device with [insert relevant job title or department here]. [insert relevant job title or department here] will record the device and all applications used by the device. Personal mobile devices can only be used for the following organisation purposes:* [insert each type of approved use such as email access, organisation internet access, organisation telephone calls etc.]

Each employee who utilises personal mobile devices agrees:* Not to download or transfer organisation, personal or sensitive information to the device. Sensitive information includes [insert types of organisation or personal information that you consider sensitive to the organisation, for example intellectual property, other employee details etc.]
* Not to use the registered mobile device as the sole repository for [organisation’s] information. All organisation information stored on mobile devices should be backed up in a way that adheres to [organisation]s’ backup strategy.
* To make every reasonable effort to ensure that [organisation]'s information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected;
* To maintain the device with [insert maintenance requirements of mobile devices such as current operating software, current security software etc.]
* Not to share the device with other individuals to protect the [organisation]’s data access through the device;
* To abide by [organisation]'s internet policy for appropriate use and access of internet sites etc;
* To notify [organisation] immediately in the event of loss or theft of the registered device

All employees who have a registered personal mobile device for [organisation] use acknowledge that the organisation: * Owns all intellectual property created on the device
* Can access all data held on the device, including personal data
* Will delete all data held on the device in the event of loss or theft of the device
* Has first right to buy the device where the employee wants to sell the device
* Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
* Has the right to deregister the device for organisation use at any time

Keeping mobile and storage devices secureIt is the employee’s responsibility to observe all mandated security practises when handling mobile computing devices (including storage devices, cell phones, notebooks and iPads):* Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away;
* Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended;
* Mobile devices must have up to date and approved anti-virus software installed at all times, with regular scans undertaken.
* Mobile devices should be carried as hand luggage when travelling by aircraft.
* Any portable storage (i.e. USB stick) must be appropriately encrypted and secured when storing [organisation] data. All data must be securely erased within a reasonable and finite timeframe, i.e. one day or one week.

ExemptionsThis policy is mandatory unless [insert relevant job title or department here] grants an express exemption in written form. Any requests for exemptions from any of these directives, should be referred to the [insert relevant job title or department here].Breach of this policyBreaches of this policy will be considered a serious matter. Employees who do so will be subject to disciplinary action, up to and including termination of employment.Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.Indemnity[Organisation] bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify [organisation] against any and all damages, costs and expenses suffered by [organisation] arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by [organisation]. |
| **Review Protocol** | Policy Owner:Policy Reviewed By: Date Reviewed: Next Review Date:  |