# Bring Your Own Device (BYOD) Policy

## Overview

A flexible and productive workplace is key to user productivity. Many staff have personal hardware devices, software applications, utilities, tools, software development kits, and related products that they would like to use in the workplace. This policy defines how staff-owned devices can be used within the [LEP] network.

## Purpose

This policy establishes the rules for use of personally owned devices and technologies within the [LEP] technology infrastructure.

## Scope

This policy applies to all [LEP] staff, users, and contractors who operate BYOD devices on the [LEP] network.

## Policy

All devices within [LEP]’s environment shall be managed to prevent security and malware incidents regardless of ownership. While [LEP] has a Bring Your Own Device (BYOD) and Bring Your Own Technology (BYOT) culture, risks related to these devices must be managed.

The [Insert the Applicable Department] under the direction of the [Insert Applicable Role] shall implement the following controls to lower and mitigate risks outside devices have on the internal [LEP] network:

* [Insert applicable department or role] shall ensure access to sensitive data from BYOD devices and technologies have strict password and encryption controls in place
* All BYOD hardware with [LEP] data must be encrypted (see the Encryption Policy for more information)
* Anti-malware software shall be used and updated on a regular basis. See the Anti-Malware Policy for more information
* The use of portable flash drives is prohibited without the express written permission of the [Insert Applicable Role]
* The [Insert Applicable Role] may identify applications, hardware, and/or technologies that, due to their sensitive nature, may not be accessed by BYOD devices and technologies
* The [Insert Applicable Role] may restrict access to [LEP] resources based on employee responsibilities, location, and/or lack of management approval
* The [Insert the Applicable Department] shall keep the [Insert Applicable Role] informed of any and all BYOD threats

In the event a device is lost or stolen, the [Insert the Applicable Department] shall quickly block access to [LEP] resources from the device and where appropriate, turn tracking or location services on for the unit to aid in recovery. In addition, the [Insert the Applicable Department] shall:

* Promptly clear [LEP] data and applications when able; and/or
* Wipe or “brick” the entire BYOD device if deemed necessary to ensure the security of [LEP] resources. Wiping the entire BYOD device may have staff implications including the inability to make calls, loss of contacts, and/or the need to have the device restored.

Use of personal devices in the work environment is a privilege and benefit, not a condition of work. The [LEP] shall not be held liable for loss of use, device restoration, operating system or software application re-installations or any other component on the device should the resource require service or reset. Staff should take the proper precautions (e.g. physical controls over devices, backing up of contacts and files, etc.) to minimize any disruptions on their personal devices.

BYOD devices and technologies shall employ controls that meet the following requirements:

* Password required at start up (power on)
* Twenty (20) minute inactivity timeout/password protected screen saver
* A regular password change frequency (per the Access Control and Password Policy)
* [LEP] files should not be stored locally on the device but on [LEP] shared storage
* Safeguards exist to ensure only approved users of BYOD devices and technologies can access [LEP] resources and data

Staff shall not:

* “Root” or “jailbreak” a BYOD device and technology to free it from pre-defined limitations or remove security/licensing/compliance features
* Modify BYOD device and technology hardware and/or software beyond installation of updates provided by the device maker or service provider
* Disable BYOD device and technology protection systems including passwords, encryption, firewalls, and anti-malware without the approval of the [Insert Applicable Department]

The [Insert the Applicable Department] shall prepare and maintain a list of authorized BYOD devices and technologies. In addition, the [Insert the Applicable Department] shall specify specific configurations and circumstances under which BYOD devices and technologies may connect to [LEP] information resources and applications.

Staff shall be responsible for adhering to the requirements of this policy. Staff shall notify the [Insert the Applicable Department or Role] when:

* A new BYOD device or technology is acquired and needs access to [LEP] resources
* A BYOD device or technology is taken out of service and is no longer used
* The staff member’s role changes requiring a change in access (e.g. a change in position or leave of absence)

Except as otherwise stated in this policy, the [LEP] assumes no financial responsibility for employee owned BYOD devices or technologies. The [LEP] shall not reimburse staff for the following expenses:

* BYOD device or technology initial cost, maintenance, or replacement
* Any recurring costs related to voice, storage and/or data usage, etc.
* Wi-Fi connectivity charges including hotspot usage
* Insurance
* Expenses related to restoring BYOD devices or technologies if lost, damaged, or corrupted (e.g. malware, incompatible applications, changes to operating system)

The [Insert the Applicable Department] shall periodically review, evaluate, update, and implement procedures and measures strictly limiting access to sensitive data from BYOD devices and technologies as required to maintain the confidentiality of personally identifiable information and confidential systems.

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of [LEP] operations. Examples of acceptable controls include:

* Access and inventory control lists of BYOD devices
* Specialized GPO and deployment strategies associated with BYOD devices
* Mobile Device Management (MDM) infrastructure and controls
* One or more segmented networks to isolate BYOD traffic
* BYOD device filtering logs
* Management communications and documentation of policy implementation either through meeting minutes or email

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff and contractors using [LEP] information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/04/2016 | Initial Policy Drafted |  |
|  |  |  |  |