Bring Your Own Device (BYOD) Policy

Effective 3/1/2017

This policy establishes Imagine! guidelines for employee use of personally owned electronic devices for work-related purposes.

Bring Your Own Device (BYOD) Mobile Devices are defined as devices that are bought and paid for by Imagine! employees and owned individually by the employee or any entity that is not Imagine!. ***These devices are NOT owned by Imagine!*** Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops, wearables, and computers.

Procedure

Eligibility

Employee eligibility will be determined by job function and management approval. The IT department holds the sole right to deny access to the company network if all conditions are not met.

Technology devices that are eligible for this service must be in compliance with Imagine! security settings on servers, able to receive updates and able to sync with Imagine! server systems that administer services to mobile devices.

Devices and support

Imagine! will provide LIMITED connectivity support for eligible employees; employees should contact the device manufacturer or their carrier for operating system, hardware-related issues or applications not affiliated with the Imagine! mobile device management (MDM) applications.

Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

Devices that are used to access company data may be required to be registered through the Imagine! MDM enrollment procedure to ensure proper job provisioning and configuration of standard Imagine! MDM applications, which may include office productivity software and security tools, before they can access the network.

Devices that cannot meet these requirements will not be eligible for support from the IT department and will be blocked from Information Technology systems.

In order to prevent unauthorized access, devices must be password protected using the features of the device which is required to access the company network. Employees will not download any application or service to their mobile device which allows the password feature to be bypassed for access to Imagine! data.

When devices are registered with the MDM application, the following restrictions will be enforced:

- The device must lock itself with a password or PIN if it's idle for 10 minutes.
- The PIN or password must contain at least 4 characters.
- After 15 failed login attempts, the device will lock. Contacting the IT Department may be required to regain access to company data.

Mobile device features and specifications are subject to change without notification due to technology changes and the sensitive nature of our business.

Rooted (Android) or jail broken (iOS) devices are strictly forbidden from accessing the network. Employees will not modify the operating system of a mobile device in any way that allows them to bypass limitations and protections Imagine! imposes as a condition of connecting to its systems.

Access to company data will be terminated if 1) the device is lost, 2) the employee or employer terminates his or her employment, 3) or IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Imagine! will not take responsibility for the employee's personal data, software, applications or hardware in the event it is remote wiped. It is the employee's responsibility to take additional precautions, such as backing up applications, music, and other personal settings.

Restrictions on authorized use

Employees whose personal devices have camera, video, or recording capability are required to follow Imagine! policies on HIPAA and confidentiality while at any Imagine! facility or function. All protected health information and other client information must be safeguarded, protected, and kept confidential. Individuals receiving services cannot be photographed, videoed, or recorded without a release completed by the individual or guardian.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Imagine! policies pertaining to harassment, discrimination, retaliation, confidential information, and ethics apply to employee use of personal devices for work-related activities.

Excessive personal calls, e-mails, or text messaging during the workday, regardless of the device used, can interfere with productivity and be distracting to others. Employees are expected to handle their personal matters on non-work time.

In accordance with applicable law, Imagine! requires non-exempt employees to obtain the express authorization of their manager or supervisor to work outside of their normally scheduled hours. Access to Imagine! information (such as email) via a mobile device does not constitute authorization to work outside of normally scheduled hours.

Employees may not use their personal devices for work purposes during certain leaves, such as unpaid leave or medical leave, without authorization from their supervisor. Imagine! reserves the right to deactivate company access on the employee's personal device during certain leaves.

Employees are responsible for ensuring that company information and data stored on or accessible from their personal devices remains secure. Employees must delete any client related data (including contact information) and other work related information from their personal device upon separation of employment. Upon separation, employees will arrange for IT to have Imagine! applications and related information removed from their phones.

Privacy/company access

No employee using her or his personal device should expect any privacy except that which is governed by law. Imagine! has the right, at any time, to monitor and preserve any communications that use the Imagine! networks in any way, including data, voice mail, telephone logs, internet use and network traffic, to determine proper use.

Imagine! may have incidental access to personal information on personal devices. In such event. Imagine! will only review, retain, release, or disseminate personal and company related data on personal devices as required by law to government agencies and its representatives in the event of an investigation or litigation. Imagine! may review the activity and analyze use patterns, as it relates to use of the personal device for work purposes, and may choose to publicize these data to ensure that Imagine!'s resources in these areas are being used according to this policy.

Company stipend

Employees authorized to use personal devices under this policy may receive an agreed on monthly stipend based on the position and estimated use of the device. If an employee obtains or currently has a plan that exceeds the monthly stipend, Imagine! will not be liable for the cost difference. Imagine! reserves the right to terminate or modify the stipend. The stipend does not constitute an increase to base pay and will not be included in any calculations of base pay.

Safety

Employees are expected to follow applicable local, state, and federal laws and regulations regarding the use of electronic devices at all times.

Employees are expected to refrain from using their personal devices while driving for work. Employees are required to use a hands free device or pull off to the side of the road and safely stop before accepting a call or texting.

Employees who are charged with traffic violations resulting from use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost, stolen, hacked, or damaged equipment

If an employee device is registered with the MDM application and the device is lost or stolen, the employee must notify the Imagine! IT department immediately.

IT will terminate access to company data upon notification of the following:

- Termination of employment
- Lost or stolen device
- Devices no longer in use by the employee

Violations of policy

Employees who have not received authorization from Imagine! will not be permitted to use personal devices to access company data.

Imagine! reserves the right to modify or disable (or both) an employee's access to Imagine! systems any time that the user violates the BYOD Policy or such a violation is reported. Imagine! may take any one or more of the following actions (in any order Imagine! deems necessary), in its sole discretion, in response to a reported or otherwise discovered violation:

- Issue verbal or written warnings.
- Suspend or terminate the user's Imagine! MDM account or service.
- Wipe all company data from the employee's device.
- Run reports on the employee's device usage of company resources.
- Capture company data from the employee's device.
- Terminate the user's employment.
- Pursue legal remedies for violations.