# Ohio Network for Innovation
# BRING YOUR OWN DEVICE (BYOD) POLICY

---

ONI grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. ONI reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of ONI's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. ONI employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

## Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of ONI.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to…
- Devices' camera and/or video capabilities are/are not disabled while on-site.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to another company
    - Harass others
    - Engage in outside business activities
    - Etc.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- The following apps are not allowed: (apps not downloaded through iTunes or Google Play, etc.)
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- ONI has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

## Reimbursement

- ONI will contribute $5 per month toward the cost of the device.
- The company will a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan, etc.
- The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

## Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.

- The device must lock itself with a password or PIN if it's idle for five minutes.
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

## Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to ONI within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device. If the device has been attacked with malware, a virus or any other suspicious attack, this should also be reported to ONI - Any other security concern with regards to company data Release of Liability and Disclaimer to Users hereby acknowledges that the use of a personally owned device on the network carries specific risks for which you, as the end user, assume full liability.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- ONI reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.