| Document ID  **310** | Title  **BRING YOUR OWN DEVICE** | Effective Date  **10/20/2021** |
| --- | --- | --- |
| Last Date of Review  **10/20/2021** | Date of Re-Review:  **2023-2024** | Date Approved by Board of Directors:  **10/20/2021** |

1. **PURPOSE**
   1. This policy establishes NEW MILLENNIUM ACADEMY (NMA) guidelines for employee use of personally owned electronic devices for work-related purposes.
2. **GENERAL STATEMENT OF POLICY**
   1. Employees of NMA may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include: iPads, tablets, laptops and computers. The use of personal devices is limited to certain employees and may be limited based on compatibility of technology including but not limited to print and software support. Contact the IT department for more details.
3. **PROCEDURE**
   1. **Device Protocols**
      1. To ensure the security of NMA information, authorized employees are required to have anti-virus software installed on their personal device(s). NMA’s IT department must verify that the software has been installed prior to using the personal device(s) while working on site. Additionally, all employees using personal device(s) will use the NMA guest network to ensure further system integrity.
      2. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees’ homes. Employees should not use unsecure internet sites.
   2. **Restrictions on authorized use**
      1. While at work, employees are expected to exercise the same discretion in using their personal device(s) as is expected for the use of company devices. NMA policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.
      2. The COVID-19 pandemic has health providers using video conferencing tools, such as Zoom and Google Duo, to assist patients. This allows acceptable use of personal devices, in accordance with HIPPA, that will allow for usage in health, wellness and/or medical meetings.
   3. **Privacy/Company Access**
      1. No employee using their personal device should expect any privacy except that which is governed by law. NMA has the right, at any time, to monitor and preserve any communications that use the NMA’s networks in any way, including data, voice mail, telephone logs, internet use and network traffic, to determine proper use.
      2. Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.
   4. **Lost, stolen, hacked or damaged equipment**
      1. Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft.
      2. In an effort to secure sensitive company data, employees are required to have all work related files remain on the cloud services which include but are not limited to Google Drive, OneDrive and Egnyte. Files that do not contain confidential and/or sensitive data may be downloaded to personal device/s. Confidential and/or sensitive data includes but not limited to files with identifiable information of students, families or staff; accounting information and operational information.
      3. NMA will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged. Employees will be responsible for repair costs of their own personal device.
      4. Employees may receive disciplinary action up to and including termination of employment for improper use of NMA information that is stored on personal device(s).
   5. **Termination of employment**
      1. Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.
   6. **Violations of policy**
      1. Employees who have not received authorization in writing from NMA management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow NMA policies and procedures may result in disciplinary action, up to and including termination of employment.