BOARD OF TRUSTEES POLICY

LIBRARY WIRELESS COMMUNICATION DEVICES

PURPOSE

This Policy establishes Euclid Public Library ("Library") guidelines for the provision, administration, and use of Library wireless communication devices, such as Library cell phones. It aims to promote safety, productivity, and the cost-effective and proper use of such Devices.

For purposes of this Policy, a wireless communication device (referred to as a "Device" in this Policy) includes all wireless communication devices owned or provided by the Library that are either handheld or worn on the body, including without limitation cell phones, personal digital assistants, and similar technologies, along with any related equipment (e.g., cases, chargers, headsets, etc.). For purposes of this Policy, a Device does not include laptop computers.

For purposes of this Policy, a "User" includes any employee who uses a Device to perform work for or on behalf of the Library.

All employees must comply with this Policy, and with all other Library policies applicable to Devices, including, without limitation, the Library's Business Information Systems Policy.

POLICY

The Library, in its sole discretion, may assign a Device to a User who requires access for business use in accordance with assigned duties and responsibilities, and the Library may direct-pay the service cost of the Device. Users who are assigned use of a Device must sign a certification to verify acceptance and to acknowledge understanding of this Policy.

All Devices and any corresponding telephone numbers are the sole property of the Library and are to be treated as such. The Library reserves the right to distribute and/or publish cell phone numbers for Devices. Use of a Device is contingent upon continued employment with the Library and continued assignment of use by the Library. The Library, in its sole discretion, may reassign Devices and/or determine that a User will no longer be assigned use of a Device.

Users should have no expectation of privacy in these Devices or their contents, including without limitation any stored data and/or use of these Devices. Users must comply with all Library requests to make these Devices available for any reason, including audit, inspection, review, return, or any other reason. Employees who separate employment (for any reason) must return the Library Device to the Technology Manager, or to the Fiscal Officer if the Technology Manager is unavailable, prior to separation.

Administration (including Assignment, Equipment, Carriers, etc.): The Library will strive to obtain the best value at the lowest cost that best meets Library needs. The Director, and/or the Director's designee(s), will interpret and administer this Policy and serve as the main point of contact in the administration of this Policy. This administration includes: assigning/reassigning Devices, including any equipment and services; selecting Devices, including any equipment and services to be used; determining suitable carrier(s) and cost-effective plans and services; activating/terminating plans and services; determining if/when changes are needed (e.g., replacement, upgrade, return, etc.); developing incidental standards and procedures to be followed (including, for example, with respect to approved applications); and all other management and

administration of Devices. The Technology Manager and/or designee(s) will provide troubleshooting and technical support, as able, to Users.

Determinations on assignment/reassignment generally are based on the role and responsibilities of the User along with other business considerations, as evaluated by the Library Director and/or the Director's designee(s), in the Library's sole discretion. Some considerations include whether the User is expected to respond to work-related matters during non-business hours (for exempt employees) or during work hours if otherwise inaccessible; whether use of a Device will improve service efficiencies; and other business considerations. Due to financial and/or other business considerations, the assignment/reassignment of Devices may be limited, and there is no guarantee that anyone (even if previously assigned use of a Device), will be assigned/continue to be assigned use of a Device.

Additional User Responsibilities: Each User is responsible for the business-appropriate use of a Device. This includes, without limitation, the following:

Business/Non-Personal Use:

- Users may use Devices only for work-related purposes, except as otherwise stated herein.
- As a general rule, Users may not use Devices for personal use. If an urgent personal issue or other incidental, occasional personal matter arises, then a User may use the Device in such instance provided the use is *de minimus* (i.e., no more than a few minutes). Other personal use is prohibited without prior approval, in advance, from the Library Director and/or the Director's designee(s).
- Users must comply with any usage limits communicated by the Library.
- Users may not use a Device to record conversations, images, or meetings, unless prior approval is obtained in writing; unless the camera feature is being used for appropriate business reasons consistent with Library procedures for using a camera and consistent with local, state, and federal law; or except in an emergency. The camera feature on a Device may not be used for personal reasons.
- Users may use a Device to report emergencies to the appropriate authorities.

Safety/Driving:

- Users must put safety first and comply with all laws (of which they should maintain awareness) at all times while using a Device.
- When driving on Library business and/or while using a Device, Users must follow all laws related to use of the Device. Users also are expected to refrain from using a Device while driving and instead should use a Device only when the vehicle is safely parked. Users who are charged with traffic violations resulting from the use of a Device while driving will be solely responsible for all liabilities and costs that result from such actions. These rules also apply with respect to employees when using any other wireless communication device while driving on Library business or when using any other wireless communication device for Library business while driving.
- Users who work in hazardous areas or who are operating equipment must refrain from using Devices, as doing so can potentially be a major safety hazard.

Compliance with Law and Policies:

- Records, including those maintained on and/or relating to Devices, may be subject to disclosure under law, may be disclosed to government agencies or third parties during investigation or litigation, and/or may be disclosed for other reasons, in the sole discretion of the Library.
- Users must follow all applicable local, state, and/or federal laws when using Devices. Users may not use a Device in an illegal, illicit, dangerous, inappropriate, harassing, or obscene manner.
- Users must comply with all other Library policies when using Devices, including but not limited to policies pertaining to harassment, discrimination, retaliation, business information systems, safety, confidentiality, public records, and ethics.

Work Hours:

- The Library may require Users to return a Device at the end of their shifts, or to leave the Device in a specified location at the Library at the end of their shifts.

- Users who are on a leave of absence may not use a Device for work purposes during the leave without prior approval, in writing, from their manager or supervisor. (The Library may require these Users to return a Device, or to leave it in a specified location at the Library, during such leave.)

Care and Security: Users must be diligent in the care and protection (including from loss, theft, or damage) of any Library Device entrusted to them. This includes:

Failure to Return, Loss, Theft, Damage, Breach:

- Prior to separation of employment (for any reason) or upon Library request (for any reason), the User must return the Device to the Technology Manager, or to the Fiscal Officer if the Technology Manager is unavailable.
- In the event of loss, theft, or damage, a User must report the situation immediately to their manager or supervisor. In some instances, the Library may require the User to report the matter to the authorities. At the discretion of the Library, a User may be responsible for the cost of the Device or the cost of repair if the Device is lost, stolen, or damaged.
- Users must immediately report to their manager or supervisor any incident, or suspected incident, of unauthorized data access, data loss, "hacking," and/or unauthorized disclosure of Library resources, databases, networks, etc.

Security Measures:

- Users must comply with all security measures required by the Technology Manager and/or designee(s). These measures may include password requirements (such as requirements that the Device be secured by a password; that the password not be disclosed to anyone other than the Technology Manager and/or designees; that the password be kept on file with the Technology Manager and/or designee(s); etc.); requirements pertaining to remote wipe software, which allows all data to be erased remotely in the event the Device is lost, stolen, or not returned as required; and any other measures required by the Technology Manager and/or designee(s).
- Users may not modify Device hardware or software or install additional hardware or software (including applications), beyond authorized and routine installation updates.

Audit/Review: Devices and their usage are subject to audit, review, servicing, and inspection at any time, and there is no expectation of privacy in these items. The Library Director, and/or the Director's designee(s), will review billing statements on a monthly basis, and they may review whether usage is appropriate and fiscally prudent. At the discretion of the Director or designee(s), Users may be required to reimburse the Library for unauthorized use.

Violations of this Policy may result in disciplinary action, up to and including termination of employment.

Adopted by the Board of Trustees 4-21-2020