POLICY: HR12 – Searches and Inspections
APPROVAL DATE: 05/15/2018
REVISION DATE:

Purpose
To set forth the District’s policies for inspections and searches of work stations and technology resources.

Scope
Applies to all District employees and volunteers

12.1 Property

The District provides work stations, including desks, files, lockers, closets, etc., to carry out legitimate District business. Users are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that would reflect negatively upon the District, Library Board, Executive Director, or media should be avoided.

By using the District’s equipment, including work stations, an employee consents to reasonable search of the work station. There is no right to privacy in the use of District equipment.

In order to maintain a safe workplace for all staff, employees of the District are advised that upon reasonable suspicion, the District reserves the right to inspect or search, without advance notice, any desk, file, locker, closet or other container provided by the District. The District may also, upon reasonable suspicion, inspect or search employee possessions present on District property, with advance notice to the employee.

Where applicable, the District will provide locks for employee use and shall retain a key or combination to all locks provided for use by employees in the workplace. Employees may not use a personal lock on District property unless authorized by the District.

Employees who do not permit the searches described above may be subject to disciplinary action up to and including termination.

12.2 Computers and Communications Systems

The District provides network, communications systems, equipment and devices (“technology resources”) to carry out legitimate District business. By using the District’s technology resources, an employee consents to disclosing the contents of any data files, information and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment or devices. There is no right to privacy in the use of District’s technology resources. By using the District’s technology resources an employee consents to monitoring, recording, and reviewing the use of that technology resource.
The District reserves the right to monitor, review, audit, intercept, access, and disclose all messages and/or data created, received, or sent over any of its electronic systems for any purpose at any time. All messages or data created, sent, or received using any of the District’s electronic communication or computer systems are considered property of the District. Only employees authorized by the Executive Director may research, retrieve, read, or copy messages and/or data stored on any of the District’s electronic systems by another user. Unethical, inappropriate, or illegal use of District computer or communication systems, equipment, or network is prohibited and may lead to disciplinary action up to and including termination.

The Executive Director is responsible for establishing administrative procedures necessary to carry out this policy and will respond to appeals of District staff action and/or decision in the application of this policy and any related procedures. Any appeal of Executive Director action and/or decision may be made in writing to the Board of Trustees.

The District will comply with all federal, state and local law regarding employment and will make a good faith effort to implement this policy in a fair and consistent manner.

In the event of the amendment of any law, regulation, or ordinance incorporated into these policies or upon which this manual relies, these policies shall be deemed amended in conformance with those changes. In cases where these policies conflict with any local ordinance, state or federal law, the terms of that law, and its underlying rules or regulations shall prevail. In all other cases, these personnel policies and practices prevail.