ADMINISTRATION BUILDING
835 OLD CLAIRTON ROAD
JEFFERSON HILLS, PA 15025
PHONE: 412-655-8450
FAX: 412-655-9544
www.wjhsd.net

WEST ELIZABETH - JEFFERSON HILLS - PLEASANT HILLS

POLICY 453 – USE OF PUSH-TO-TALK COMMUNICATION DEVICES

1. Objective

The School Board supports the use of push-to-talk (PTT) communication devices within the District as a means to enable effective and reliable communication between designated District personnel. The District authorizes use of push-to-talk devices for the following purposes, but such use is not necessarily limited to:

- Coordinating fire drills;
- Coordinating emergencies/building evacuations;
- Security issues;
- Coordinating special events/sporting events, including parking;
- General communication between principals and office/building staff;
- General communication between facilities' staff.

2. Scope

This policy applies to all District staff authorized to use push-to-talk devices.

Primary uses of the push-to-talk devices are the school principals, school principal designees (such as office secretaries, school nurses, head teachers, etc.), security officers and facilities' staff. As needed, other staff may use the devices upon approval by the appropriate school principals or the Director of Facilities.

3. Policy

Authorized personnel may only use District push-to-talk communication devices for approved purposes in prescribed manners consistent with all District policies.

4. Standards

a. Push-to-talk (PTT) devices are to be used for District purposes only, and not for any employee's personal business or communications.
b. PTT devices assigned to a specific school are to remain at that school unless authorized by the school principal or Director of Facilities for offsite use.
c. Cellular calls are to be avoided if push-to-talk correspondence is available.
d. Cellular calls must not exceed 400 minutes per month per PTT device.
e. Software and applications must not be installed on the PTT device unless authorized by the Director of Facilities.
f. Any issue with, or damage to, the device must be reported immediately to the school principal/Director of Facilities.
g. If equipped with a camera, the camera feature must not be used without explicit

approval by the school principal/Director of Facilities.

h. All pertinent safety guidelines must be followed when using the PTT device in a moving vehicle or operating machinery.
i. Employee acknowledges that his or her portion of the monthly bill may be reviewed at the discretion of administration.
j. All calls must comply with existing and future protocols for proper communication.
k. All PTT devices must comply with the existing and future guidelines listed in the Information Security and Telecommunications Acceptable Use Policies.
l. Authorized users are to place PTT devices in their designated charging stations after use and/or at the end of each work shift.

5. Reporting

All violations or non-compliances with this policy (and/or any applicable sections of the Information Security, Acceptable Use or related policies) must be reported to the Director of Facilities, IT Management and/or the Superintendent's office immediately. Failure to do so implies cooperation with the noncompliance and may subject an employee to the same consequences as the violator.

6. Consequences of Inappropriate Use

The violator of the Use of Push-To-Talk Communication Devices Policy (and all applicable sections of the Information Security, Acceptable Use or related policies) will be responsible for damages to equipment, systems and software resulting from deliberate or willful acts. All District policies, administrative procedures and communicated expectations regarding behavior and communications apply when using the telecommunications/computing environments, including such policies, procedures and expectations related to privacy, harassment, vandalism and theft.

For purposes of this policy, vandalism is defined as a malicious attempt to inappropriately access, harm or destroy data, hardware or software including parts of the District's telecommunications/computing environments or launching such an attack against another from the District's network. This includes, but is not limited to, creating, uploading or accessing viruses, installing worms or Trojan horses, launching attacks or inappropriately monitoring or capturing another user's or system's activity or data. In the event that a staff member violates any of the District's security measures, the Incident Handling Policy shall control investigation of any such incident.

A substantial charge of non-compliance against a staff member shall subject such staff member to restriction of use or access to computer/telecommunications resources and/or other disciplinary action up to and including discharge. Illegal use of the telecommunications/computing environments, deletion or damaging of files or data, copyright violations, theft of services, hacking or bypassing security controls, violations of the privacy standards of another user, student, staff or the District, or misrepresentation of another identity, or vandalism, will be reported to the appropriate legal authorities for possible prosecution.

Created July 12, 2012
Adopted July 23, 2012