Employee Use of Personal Technology on District Property

Goal: The District will allow employees to bring personal technology equipment onto school grounds to be used for personal or student needs. This document is intended to provide guidelines for the use of such equipment on the District property and over the District network.

Guidelines:

1) Personal equipment brought onto school grounds is the sole property of the owner. The District assumes no liability for any occurrence that causes damage to the equipment.
2) The District will not provide support for any personal equipment. Any issue that arises is the responsibility of the owner to resolve.
3) The District retains the right to reduce capacity and/or limit the number of users on its network at any given time. This may result in limited or no connectivity.
4) The District retains the right to pursue corrective action in an instance where a personal technology device causes damage to District owned equipment or resources.
5) There should be no expectation of privacy regarding the contents of computer files or communication undertaken by way of the district computers and/or network.
6) The District will cooperate with local, state, or federal officials in any investigation related to suspected illegal activities conducted through the district computer systems.
7) If at any time it is determined that the use of personal technology conflicts with the regular District activities, the District reserves the right to require that the employee remove said technology and refuse its use on the property.
8) It is encouraged that individuals who leave personal technology in a district building have personal insurance to cover loss and/or damage of the device/equipment.
9) Web-enabled personal technology will only have access to the guest network and will not be able to print.

If an employee of the District chooses to utilize personal technology on school property, by default, the Employee agrees to:

1) Be responsible for keeping all passwords and accounts secure.
2) Not attempt to access the District’s or other people’s files or accounts or by pass the District’s security measures.
3) Not intentionally waste or disrupt District technology resources.
4) Allow the School and District Administration to conduct an individual search of an employee’s computer files, music, video, email or other related items when being used in a student environment.
5) Ensure that the computing device is virus free by having it analyzed by the District IT Department before it is deployed over the network.

Last Updated 10/3/2011