PERSONAL COMPUTING AT SCHOOL
614

Rationale:
CISDV provides computers to staff for their basic requirement. However, some staff may prefer to use personal devices for ease of use, familiarity, or other reasons. While this may be convenient for the staff member, support of these devices is as varied as the devices themselves. The portable nature of staff owned devices has security and privacy implications as well as support and resource costs at the schools. Because of all of these concerns, some limitations on their support and use may put in place to address these issues.

Policy:
Personal equipment such as computers, tablets, e-readers, and smart-phones are permitted for staff use at schools. Access to the schools' network and network resources may be limited, and they are not permitted where security or privacy of data is of concern. Aside basic user documentation for local access, support of these devices will be the owner's responsibility.

Regulation
Where permitted, staff personal computing equipment (desktop computer, laptop, tablet, smartphone, etc.) is subject to a number of limitations and regulations on its use in the school environment. These are to make sure that the staff personal equipment does not interfere with the operations of the regular school equipment, does not require additional support resources, and the school remains in compliance with all external regulations and legislation.

1. **Personal equipment is the responsibility of the owner.**
    a. Staff computers are provided for professional use. While the school may chose to provide services for personal equipment, these are provided as resources allow, and on a best effort basis.
    b. Documentation may be provided for use of school-supplied resources by personal equipment for most common uses, but support of the device itself is the owner's responsibility.

2. **Access to School-supplied resources**
    a. As school resources permit, staff may be granted access to Internet, File or Printing services. Not all schools will provide any or all of these resources, and they maybe limited by bandwidth, time and location within the school.
    b. Access to any or all of these resources may be controlled. A staff

member may be required to register or authenticate a device in order to gain access to any resource. The form this takes may vary from school to school.

c. The device may be vetted for security, anti-virus software, or other issues that may destabilize the schools network or resources before being granted to any resource.
d. A signed agreement may be required to allow access.

3. Copyright and legal use

a. All software, images, and other content on staff owned devices used for instructional purposes must not violate copyright laws
b. At no point are these machines to be used for any illegal activity. This can include copyright violation (including file-sharing), unauthorized access of other systems (hacking), distribution of illegal content, or violation of any other laws or regulations.

4. Security of the device

The owner of the personal device will be solely responsible for their device and the school does not accept responsibility for damage, loss or theft while it is in use at the school. Owners should take necessary precautionary measures to safe guard their devices, such as not leaving the device unattended in open classrooms, visible in a parked car, etc.

5. Privacy and Security of data

a. Though the devices may be personal in nature, data developed and used for CISDV purposed are property of CISDV.
b. Schools' confidential information must not be kept on a personal portable device.
c. Due to the nature of network operations, IT staff may be able to monitor network activity on a CISDV site. Privacy of personal communications is not guaranteed.

6. Backup of data

a. Schools may choose to provide backup services for CISDV information on personal portable devices. This could be on-site, network shares, "cloud" storage, external storage (USB or data cards), or any combination.

b. Notwithstanding a., the owner of the device should also take steps to make certain their data is backed up, including periodically checking that the integrity of their backed up data.

7. Violation of policy

Any device found in violation of this policy and any of it's regulations, or otherwise causing issues for the rest of the school community, will have it's access removed. Once the device has been restored to compliance, access may be granted upon review.

Approval of specific exceptions to regulations:

Exceptions to this policy and/or it's regulations may be granted. The need for the exception must be clearly documented and be acceptable under the law. Exceptions will be granted by the IT manager, in consultation with one or any of the school principal(s) involved, the superintendent, and the IT steering committee.

Privacy and security statement

All communications are subject to Privacy legislation (FOIPOP and PIPA) as well as other CISDV policies.

By law in Canada, all business-related communications are property of the business (CISDV, in this case) and though there is some expectation of confidentiality (that communications will not be re-diverted or used inappropriately), they cannot be considered truly private.

Reference:	Approved Date Approved: March 2013
Cross-reference:	Date(s) Revised: