The following procedures are intended to outline the acceptable use of computer equipment in Pine Creek School Division, and they apply to employees, support staff, consultants, temporary staff, and other workers at Pine Creek School Division including all personnel affiliated with third parties and to all equipment that is owned or leased by Pine Creek School Division.

General Use and Ownership

a) All data created on Pine Creek School Division systems remains the property of Pine Creek School Division. Because of the need to protect Pine Creek School Division's network, administration cannot guarantee the confidentiality of information stored on any network device belonging to Pine Creek School Division.
b) Employees are responsible for exercising reasonable judgment regarding the personal use of Division technology.
c) For security and network maintenance purposes, authorized individuals may monitor equipment systems and network traffic at any time.
d) Pine Creek School Division reserves the right to audit networks and systems on a periodic basis to ensure compliance with these procedures.
e) Should an employee wish to have a private means of accessing their personal email accounts/other communications, including any access to the internet for personal reasons, employees are advised to do so by using their own electronic device and not through a connection to the employer's network.
f) Employees are advised that, during business hours, the use of personal technology devices such as cell phones ought to be limited to work-related endeavors that coincide with Pine Creek School Division's policies and procedures and should in no way interfere with the employee's responsibilities relative to their specific job descriptions.

Security and Proprietary Information

a) The information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Employees should take all necessary steps to prevent unauthorized access to information of a confidential nature.
b) Authorized users are responsible for the security of their passwords and accounts.
c) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
d) In order to prevent the unauthorized or inadvertent disclosure of sensitive or personal information, employees must exercise caution when sending any email from inside Pine Creek School Division to an outside network.
e) All employees are responsible for ensuring periodic review and clean-up of their individual email files to avoid undue overload on the system.
f) All employees are responsible for ensuring periodic review and clean-up of their files stored on school servers to avoid undue overload on the system.
g) Data storage quotas may be implemented to avoid undue overload on the system.

Unacceptable Use

Under no circumstances may Pine Creek School Division-owned resources be used to engage in any activity deemed illegal under provincial, federal or international law. Other prohibited activities include

a) Violations of the rights of any person, organization or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

b) Unauthorized copying of copyrighted material including installation of any copyrighted software for which Pine Creek School Division or the end user does not have an active license.
c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
d) Introduction of malware programs into the network or server.
e) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
f) Using a Pine Creek School Division technology asset to actively engage in procuring or transmitting material that is in violation with sexual harassment or hostile workplace laws in the user's local jurisdiction.
g) Making fraudulent offers of products, items, or services originating from any Pine Creek School Division account.
h) Making statements about commitments/guarantees, expressly or implied, unless it is a part of normal job duties.
i) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user's host computer, via any means, locally or via the internet/intranet/extranet.
j) Providing information about, or lists of, Pine Creek School Division employees to parties outside Pine Creek School Division**.**

Prohibited email and communications activities

a) Any email communications related to employment at Pine Creek School Division must be via email accounts approved by the Manager of Information Technology.
b) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
c) Any form of harassment via email, telephone, paging, or text message whether through language, frequency, or size of messages.
d) Unauthorized use, or forgoing, of email header information.
e) Creating or forwarding "chain letters", "pyramid" schemes of any kind.

Guidelines on Anti-Virus Process

a) Always run Pine Creek School Division standard supported anti-virus software.
b) Download and install anti-virus software updates as they become available (typically this process is automated).
c) NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
d) Forward any spam, chain, and malicious email to spamreport@merlin.mb.ca, then delete the email.
e) Never download files from unknown or suspicious sources.
f) Avoid direct disk sharing with read/write access unless there is absolutely a requirement to do so.
g) Always scan USB drives from an unknown source for malware before using it.
h) Back-up critical data and system configurations on a regular basis and store the data in a safe place.
i) If the anti-virus software is disabled, inform the IT department immediately and refrain from using the computer until the anti-virus software has been enabled.