Administrative Procedure 805 – Appendix A

Accessing Computers – Acceptable Use Protocol

Part I: Staff Conditions of Use

It is important for staff members to be aware of the operational conditions under which computers and computer networks are made available to them. The following information applies to teachers and support staff.

a) Access to and use of Division computers and the computer networks may be monitored.
b) Files or electronic communications involving the use of Division computers or computer networks are not considered private.
c) Computers and Division computer networks are available only to users who act in an ethical, responsible, legal and professional manner.
d) Computers and networks must be used for work-related and acceptable purposes, as outlined in the Acceptable Technology Use Continuum (Appendix B)
e) A breach of the conditions of use or guidelines may result in a temporary or permanent suspension of computer privileges or other sanctions.

Part II: Staff Guidelines

It is expected that staff will utilize Division computers in a professional manner with due regard to the following:

a) Preservation of the privacy of login (ID) and passwords.
b) Preservation of the security of systems, material, and information to the highest degree possible.
c) Reporting of known security breaches to a supervisor or network administrator.
d) Avoiding the sending, viewing, or distribution of offensive, inappropriate, or harmful material.
e) Honoring copyright laws and license agreements, including digital resources, streaming services, and software.
f) Using Division network resources responsibly and avoiding excessive non-work-related bandwidth use (e.g., streaming media, gaming).
g) Recognition that the content of any and all uploaded material reflects on the image of the school division.
h) Forfeiture of the right to use Division infrastructure for personal financial gain.
i) Required notification and approval of the network administrator prior to making any changes to the setup of school computers.
j) Ensuring that all external media (e.g., USB drives) are scanned for viruses before use on a Division computer.
k) As an employee, the use of personal electronic devices during assigned work hours should be limited to emergency situations or as necessary to perform work-related tasks. Personal phone calls or texts should be avoided during assigned work hours. Employees must also ensure that their cell phones are secure and protected with a passcode or password to prevent unauthorized access to school division data.
l) All employees are strongly encouraged to complete assigned network security training modules.

I have read and understood the conditions of use and the guidelines of this Acceptable Use Protocol.