Administrative Procedure 140 – Appendix B

NEXT GENERATION NETWORK (NGN) ACCEPTABLE USE STANDARDS

Background

District internet use procedures require responsible and appropriate use of network resources. Because the Next Generation Network (NGN) is part of the provincial government network, similar standards of use apply. The purpose of this administrative procedure is to clarify acceptable use standards and appropriate educational uses of the NGN.

1. To manage network capacity and ensure optimal performance of the network, please consider:
   1.1. Rich multimedia websites, including radio stations and video services, can enhance the classroom. Similarly, multi-player network games such as Minecraft and others can enrich the learning experience for students. However, the use of such services is to be education related.
   1.2. Limit the download of large files, such as movie or music files, unless they are education related. Downloading large files impacts network performance. Consider providing a link to these resources hosted on storage sites such as YouTube instead of downloading. In addition, be wary of copyright laws that may prohibit the downloading and distribution of the content.

2. To safeguard the security of the network for all students, staff and guests:
   2.1. Be suspicious of all emails particularly if they contain attachments. Avoid opening attachments whose origin appears questionable. Delete such emails immediately. These emails often contain viruses that can disrupt or seriously damage the target computer. Do not respond to emails asking for your login credentials (i.e. username/password) as these emails are intended to steal your identity. The District employs anti-virus/spam software to protect users but occasionally these malicious emails do get through. The exercise of caution and a little skepticism is the best defense.
   2.2. Avoid downloading any files from non-reputable sites. As in clause 2.1 above, exercise caution and skepticism as downloaded files may contain malicious payload disguised as a useful program (Trojan horse). If unsure of the legitimacy of a website or its content, please contact the IT Service Desk for assistance.
   2.3. District staff and students are expected to use their District-provided email accounts when corresponding with other staff and/or students. The use of this service and the content therein are governed under Administrative Procedure 140: Computer Access to Electronic Information and Administrative Procedures 146: Use of Social Media.

3. For more information, questions, or assistance contact:
   IT Service Desk at 250-377-HELP

Reference: Sections 17, 20, 22, 65, 85 School Act
Freedom of Information and Protection of Privacy Act
School Regulation 265/89

Adopted: December 15, 2020