5019: TECHNOLOGY ACCEPTABLE USE (AP)

ADMINISTRATION PROCEDURES

The Board of Education recognizes that the use of technology is an integral tool in providing meaningful, engaging and relevant educational programs as well as maintaining and providing for effective and efficient business and management functions.

As technology is ever-changing and largely unregulated, it is important for the Board of Education to inform students and staff of the risks and benefits, and to impose governance on the use of technology within the school district technology environment.

Benefits

The use of computers, mobile devices, software, networks, the internet, online communications and other technologies (collectively referred to as 'technology') provide opportunity to enhance and engage students in educational opportunities as well as provide staff with avenues for research, communication and planning. The intent of technology in the school district is to:
- Support and enhance the delivery of educational services to students and provide options to meet their learning styles, access requirements and program needs
- Provide tools to improve the efficiency and effectiveness of the business of education
- Enhance opportunities for staff to participate in professional learning activities
- Enhance communication throughout the system

System Security and Integrity

Security of the district's network and technology and of users accounts is critical to ensuring overall integrity and workings of the entire technology system. With this in mind it is expected that:
- Users not share their passwords and logon information
- Software and hardware are treated with respect and are not willfully damaged in any way
- System administrators may set limits on usage time, storage space and access
- Users will pay due diligence to ensuring that viruses and malware do not infect the network

Privacy and Confidentiality

The technology network and system of the school district is school district property and as such is not absolutely private with respect to concerns regarding misuse or contravention of this AUP. As well, it is expected that the use of district technology and networks not compromise the Freedom of Information and Protection of Privacy Act. In particular, it should be noted that:

- The school district may monitor or review individual accounts or browsing history should there be a suspicion of misuse or misconduct. RCMP may be involved where appropriate.
- Staff and students shall not post or discuss online, personal information or work related issues including student work, without the permission of all parties involved (including parents).
- When using social media or other websites to enhance classroom education or conduct School District business, personal information including full names may not be posted unless authorized and appropriate measures should be taken to protect the privacy of individuals and content where applicable.

Plagiarism/Copyright/Licensing

- Students are required to properly credit internet sources.
- Staff must abide by all copyright laws
- Only authorized and licensed resources may be shown to students as part of an educational program

Expected Behaviour on Social Media Websites

- It is suggested that 'friending' students and parents be restricted to purposes only of enhancing communication regarding education programs.
- Teaching staff must at all times conduct themselves appropriately when using social media whether it is work related or not in line with the *Standards for the Education, Competence and Professional Conduct of Educators in BC* as provided by the Teacher Regulation Branch
- Refrain from commenting on your teacher, employer, supervisor or co-workers
- Refrain from posting inappropriate comments

Unacceptable Use

- Transmit any materials in violation of Canadian laws
- Duplicate, store or transmit pornographic materials including sexting
- Transmit or post threatening, abusive or obscene material
- Threaten, intimidate, bully or spread rumours about another individual or group
- Use anonymous proxies to get around content filtering
- Use district technology resources or the network for personal business, product or service advertising or political lobbying
- Downloading or playing non educational media or games
- Harass others with unwanted email or spam