School District #62 (Sooke)

ACCEPTABLE USE OF TECHNOLOGY	No.: B-117
	Effective: Mar. 12/19 Revised: Reviewed: Jan. 8/19; Jan. 22/19; Mar. 12/19

ADMINISTRATIVE REGULATIONS

NOTE: There must be a mechanism in place to review and approve appropriate online resources (i.e. Facebook, blogging, vlogging)

1. Responsibilities

a. The Acceptable Use of Technology policy and related regulations apply to all users of District and personal technology.
b. Principals and managers will ensure that Acceptable Use of Technology Policy and Regulations are reviewed annually by users.
c. Principals and managers will ensure that guardians are reminded annually of Acceptable Use of Technology Policy and Regulations, including where they can be found for review.

2. System Administration and Management

a. The system administrators are authorized to block access to or remove content from District technology that is in violation of District policy.
b. With regard to the District's information systems:
   - At the request of a principal, where there is reasonable belief that this policy has been violated, system administrators shall access a history of the student's activities.
   - System administrator will not access a staff member's history of activities except as follows:
     - with the explicit permission of the staff member, or
     - upon the written instruction of the Superintendent of Schools, or
     - where required by law, or
     - where such access is reasonably required to prevent a significant threat to personal or public safety

3. Usage and Technology Etiquette

a. The District expects that the use of district or personal technology for the purpose of supporting educational programs and the District's administrative services will occur in an ethical, responsible, and legal manner.
b. The use of District or Personal technology in relation to a school district related activity must not result in a threat to the safety and welfare of students and/or employees or any other member of the school community.
c. All users of District technology are expected to follow all District policies and regulations. Students must also ensure that their use of District technology

is consistent with the guidelines and expectations outlined in the school's Codes of Conduct.

d. Users are responsible for using District technology in a secure manner. They must keep their password confidential and must not share passwords.
e. The District is not responsible for the loss of any data or information related to the personal use of District or Personal technology.

4. District Approved Electronic Learning Resource/Communication

a. Use of electronic learning resources must be in accordance with Policy and Regulation B-115 - Learning Resources
b. Communications:
    - All employees are provided with a District email account (sd62.bc.ca) which is approved for all legal, electronic communication related to an employee's performance of duties
    - Employees may have a second District approved email account (sd62learns.org), approved only for communication between sd62learns.org accounts and with sd62.bc.ca accounts
    - Students may be provided with an sd62learns.org account. The use of this account by students will be governed by a Privacy Impact Assessment
    - Employees may communicate electronically with additional tools as approved by a committee authorized by the Board for this purpose

5. Prohibited uses of District technology include:

a. Transmitting or possessing any materials in violation of Canadian laws;
b. Intentionally receiving, viewing, duplicating, forwarding, storing, or transmitting pornographic materials;
c. Transmitting, posting, or linking to disrespectful, derogatory, offensive, threatening, harassing, discriminatory, abusive, obscene, or illegal messages, materials, activities;
d. Intentionally duplicating, storing, installing, or transmitting any digital material that contravenes the *Copyright Act*;
e. Plagiarizing any information obtained through District technology, or any other means;
f. Participating in online gambling sites;
g. Forging any document or message; obscuring the origin of any message, transmission, or file;
h. Using programs that harass users; prevent access; investigate, intercept, examine, or infiltrate computer systems, information, or software components;
i. Engaging in any other conduct that would be a reasonable cause for discipline.

6. Privacy

a. The District will not intentionally access, use, or disclose personal information except when:
    - disclosure is required as part of a misconduct, or investigation or in relation to a breach of law

- disclosure is required as part of a misconduct, or investigation or in relation to a breach of policy;
- there are compelling safety or security concerns, or
- the Board is legally authorized or compelled to do so.

b. In the course of maintaining the health, performance, and recoverability of District technology, network transmission patterns and statistics (not content) are routinely monitored, and information and data (content) are routinely backed-up.

7. Violations of Policy

Violations to this policy may result in privileges relating to District technology being restricted, suspended, or revoked and may result in disciplinary action.

Violations of this policy may be reported to the appropriate law enforcement authorities and may also be subject to criminal investigations and/or criminal charges.