Y.   **Cyberconduct and Cyberbullying**

1.   **Definitions**

a)   Appropriate cyberconduct involves a set of guidelines for behaving appropriately online including all forms of electronic communication. In an educational setting, examples of appropriate cyberconduct include:

i)   maintaining professional standards when communicating with teachers, students, parents, and administrators;

ii)   maintaining the confidentiality of information about students, parents, teachers, or administrators;

iii)   respecting the rights of all members of the online community and acting in a manner that facilitates the orderly functioning of that community;

iv)   ensuring that appropriate safeguards and privacy protection measures are in place prior to posting personal or professional data.

b)   Cyberbullying: The use of information and communication technology to bully, embarrass, threaten or harass another. It also includes the use of information and communication technology to engage in conduct or behaviour that is derogatory, defamatory, degrading, illegal, and/or abusive.

c)   Information and Communication Technology (ICT): Equipment including, but not limited to, current and emerging stationary or wireless technologies or systems that can be used by individuals or groups for the purpose of communication, entertainment, data management, word processing, internet access, image capture/recording, sound recording and information transmitting/receiving/storing.

d)   Safe School Environment: Within the context of cyberconduct, it is an environment where teaching and learning takes place while accessing and utilizing all the educational opportunities, influence and potential of information and communication technology. Furthermore, it is a setting that is equitable and free from hazards and abuses directed at, or occurring from, users of information and communication technology.

2.   **Guiding Principles**

a)   Safe and caring schools that promote healthy workplaces for teachers and healthy learning environments for children and youth should be a provincial and school district priority.

b)   Collectively, society shares the responsibility for creating positive learning environments that include cyberspaces which foster respect and understanding, and are free from inappropriate cyberconduct including cyberbullying.

c)   Individual rights to freedom of information, thought, belief, opinion and expression, should be balanced with the rights and responsibilities of parents, guardians and the education community. These include the right to guide individuals in the responsible use of information and communication technology.

d) Any response to cybermisconduct and/or cyberbullying should focus on protection of students, teachers, and the school community.

e) Cybermisconduct, including cyberbullying, negatively influences student learning and teacher workplaces and should be viewed as a significant occupational health and safety issue.

f) Cybermisconduct that originates from the school or from the community at large, which ultimately has a negative impact on the school climate and/or culture, warrants immediate and decisive action by the school board/district, including the imposition of sanctions, when appropriate, on the offender(s).

g) Swift, decisive action is necessary to effectively respond to cybermisconduct and/or cyberbullying. Varied strategies and responses are required to address this complex, multifaceted problem.

3. **Education**

a) Education, the most effective preventative measure to combat cybermisconduct and/or cyberbullying within school communities, is a shared responsibility of students, teachers, parents, administrators, school districts, communities, site administrators and the NLTA.

b) Education for cyberbullying prevention is a necessary and key element in addressing and preventing cyber-related harm. It promotes positive, rewarding cyberexperiences and constructive interactions in an educational setting.

c) Anti-bullying principles form the basis for appropriate cyberconduct and cyberbullying prevention. Education should involve:

   i) modeling and demonstrating appropriate cyberconduct;

   ii) utilizing a whole school/whole community approach;

   iii) focusing on prevention, protection and intervention and, where possible, a restorative justice approach for violations.

d) Teachers and members of the school community, including parents, should have ongoing access to learning opportunities that provide current, relevant education about evolving information and communication technology resources, appropriate cyberconduct and cyberbullying prevention strategies. Programs should be offered by multiple stakeholders.

e) Principles, processes and actions for effective cyberconduct and anti-cyberbullying education include:

   i) developing educational materials in partnership with all stakeholders;

   ii) disseminating educational materials about appropriate cyberconduct to the school community in its entirety;

iii) recognizing that educators, teachers, students, parents and the entire school community, including service/site providers, have a responsibility in working to eliminate cybermisconduct and cyberbullying from the teaching and learning environment;

iv) ensuring materials and information contain details that recommend guidelines for safe and appropriate cyberconduct, and outline recommendations for response if targeted by cybermisconduct;

v) establishing consequences for engaging in cybermisconduct and/or cyberbullying that negatively affects the school climate and/or culture.

f) Teacher preparation programs should include:

i) comprehensive and current information about appropriate cyberconduct and cyberbullying prevention measures. This should include data, facts and realistic examples of occurrences;

ii) lesson plans and strategies that assist teachers to recognize and address cybermisconduct and cyberbullying in classrooms and school communities;

iii) information and practical experience with new and emerging information and communication technology, including instruction regarding the appropriate educational use of ICT and professional conduct in all forms of electronic communications.

4. **Roles and Responsibilities**

a) **Students**

i) At home, at school and anywhere outside the school, students should follow principles of appropriate cyberconduct and adhere to principles and policies of acceptable use.

ii) Students should advise the appropriate adult if they observe/know about another person being bullied or experience bullying themselves.

iii) Students are encouraged to actively participate in and contribute to school districts' cyberconduct and anti-cyberbullying activities including policy development and education programs.

b) **Parents and Guardians**

i) Parents are encouraged to:

- promote appropriate cyberconduct and anti-cyberbullying behaviour at home;

- familiarize themselves with the information and communication technology and websites used by their child;

- have an acceptable use agreement for the use of information and communication technology at home, which includes clearly identified and consistently enforced consequences;

- keep computers and other information and communication technology devices in an open, common area and have filter software installed;

- determine if the school district has a cyberconduct and/or anti-cyberbullying policy and review its contents. If such policies are not in place, parents should pursue having one adopted through their local school council;

- actively participate in and contribute to school district cyberconduct and anti-cyberbullying activities including policy development and education programs;

- maintain open communication with children about appropriate cyberconduct and/or cyberbullying and treat any report(s) of bullying as a serious matter;

- become familiar with and be alert for indicators that a child may be the target of a bully.

ii)   If a child is the target of a bully, parents should assist him/her in determining the best response. Consult with the school district re the district's cyberconduct and anti-cyberbullying policy and with the school staff for assistance.

c)   **Teachers**

Teachers should:

i)   model appropriate cyberconduct;

ii)   teach appropriate cyberconduct as it pertains to any ICT used in their classrooms;

iii)   adhere to the NLTA Code of Ethics, and the school district's appropriate cyberconduct and cyberbullying prevention policy;

iv)   always maintain a professional demeanor in electronic communications with students, parents, colleagues and administrators;

v)   exercise extreme caution in any use of home computers, personal e-mail accounts and/or other personal ICT for work related contact with students or parents;

vi)   maintain appropriate professional boundaries at all times in electronic communications with students or parents;

vii)   exercise extreme caution with respect to participating in and sharing personal information and images electronically through blogs, chat rooms, social networking sites and all other forms of electronic communications/ICT;

viii)   participate in available professional development opportunities regarding appropriate cyberconduct, cyberbullying prevention and responses to cyber-misconduct and cyberbullying;

ix)   assess and appropriately respond to incidents of cybermisconduct and/or cyberbullying among students or between student(s) and the teacher.

d) **Schools, School Districts**

Schools, school districts should:

i)   collaboratively develop and adopt appropriate cyberconduct and anti-cyberbullying policies and procedures and fully communicate them to all members of the school community;

ii)   enable students and teachers to actively participate in and contribute to school district cyberconduct and anti-cyberbullying activities including policy development and education programs;

iii)   develop principles of effective, appropriate cyberconduct and cyberbullying prevention policies and procedures that include:

- an "Acceptable Use Agreement" with an attendant monitoring, evaluation, and complaints process;

- clear, comprehensive definitions of appropriate and inappropriate cyberconduct, established access privileges and identifiable consequences for those who engage in cybermisconduct;

- an explanation of the responsibilities of students, teachers, parents, and school boards with respect to appropriate cyberconduct;

- a statement that policies and procedures shall apply to any and all cybermisconduct and cyberbullying that negatively affects the school environment regardless of whether it originated from the school;

- dedicated timelines for policy and procedures to be updated regularly.

e) **Department of Education**

The Department of Education should promote and publicly advocate for appropriate cyberconduct and anti-cyberbullying behaviour in the school community by:

i)   developing and providing curriculum documents, training programs, policy and directives, and public education resources about appropriate cyberconduct and evolving information and communication technology;

ii)   amending the Schools Act, 1997 and regulations to recognize the influence of ICT and to provide explicit protection for teachers and students against cybermisconduct and cyberbullying;

iii)   providing sufficient resources to enable school communities to combat cybermisconduct and cyberbullying;

iv)   conducting its own research, or collaborating with ongoing research, about appropriate cyberconduct and cyberbullying. **[Nov24/11] [JC/Nov/11] [2013 BGM]**