Communication and Information Technology (CIT)
Expectations for Students
September 2017

The Public Schools Branch has received notification from the Department of Education, Early Learning and Culture paper copies of the Computer and Information Technology Expectations for Students and the associated Responsible Use Agreement will not be distributed to schools for distribution to students in the 2017-2018 school year. The Department will be reviewing and updating the former requirements in consultation with the Public School Branch to ensure that the policy framework respecting communication and information technology use in schools is current and effective.

If you have any questions or concerns regarding this matter, please contact your student’s teacher or the principal of your child’s school.

* * * * * * * *

Parents/guardians are asked to review the following expectations carefully with their child. Students should be encouraged to ask their parents/guardians or teacher about any parts that they do not understand.

1. Students may use electronic information for research purposes if they acknowledge the source in writing and if they respect the copyright and terms of use.

2. Students must protect their password and username and not give them to anyone else. They must not use other people’s passwords. They must also always log out of any program or Internet site after use.

3. Students must not give out any personal information to any person or system on the Internet unless it is part of an educational activity under the supervision of a teacher.

4. Students must use their Google Apps for Education account (email, online documents, calendar, video, etc.) for educational purposes. Because Google content may be housed in various countries, students must make informed decisions about what kind of information they choose to store and transmit.

5. Students may access online or offline digital resources and storage drives only according to school rules. For example, databases, Internet based resources, USB storage devices or network drives.

6. Students must not use any electronic communication device to access sites that contain or promote pornography, racism, hatred or any other inappropriate material.

7. Students must not use any electronic communication device for illegal activities, to harass (cyberbully), or for any activity that would violate the school’s code of conduct.

8. To help provide a safe environment, students or their parents/guardians must tell a counselor, teacher, or administrator about any information or messages students receive that are threatening or hurtful. They should keep or print copies of email or text messages, pictures, or any other offending materials.
9. Students must not do anything to manipulate, alter, damage, disable, or destroy the computer system, software, network, or data. Students must not do anything to circumvent the security measures provided at the school or alter the level of access permissions they have been granted.

10. Students must not use CIT in any way that interferes with other users. For example, streaming unnecessary multimedia or sending spam.

11. Parents/guardians may request access to their child’s school accounts, including email, documents and sites.

12. Students may be permitted to bring their own personal computing device which may be able to connect to the school’s wireless network. Students must follow the same guidelines regardless of the wireless network used (ie, student’s own data plan).

13. Students must only use their own device at school with the teacher’s permission.

14. Students should use up-to-date virus protection software on applicable devices.

15. Students must turn off all peer-to-peer (music, video, file sharing..) software or web-hosting services on their device while connected to the school’s wireless network.

16. The security, care and maintenance of student owned devices are the student’s responsibility.

17. The school is not responsible for the loss, theft or damage of student owned devices while at school.

18. In certain circumstances, school staff may have authority under the Education Act to search or seize school or personal devices used by a student when there are reasonable grounds to believe that a student has used CIT in a manner inconsistent with the expectations outlined herein or school rules.

Result of Misuse

Unacceptable use of CIT by a student may result in disciplinary measures by school staff including, but not limited to, restriction or cancellation of the student’s access to CIT. School staff may also contact police respecting unacceptable use of CIT by a student. Unacceptable use may include but is not limited to, audio and video recordings or photographs that violate the privacy of others, issues regarding bullying, etc. The student’s supervising teacher, the school administration, the Public Schools Branch or the Department of Education, Early Learning and Culture can decide what is unacceptable use. Students, parents/guardians should also be aware that disciplinary measures may result when a student’s off-campus CIT use has a direct negative impact on the school community.

Liability

The Public Schools Branch, the Department of Education, Early Learning and Culture, schools and supervising teachers are not responsible for any damages a student or other user may suffer arising from loss or damage of personal devices, and/or loss of data due to delays, non-deliveries or service interruptions.
Reasonable and appropriate precautions are taken to supervise and monitor student use of CIT. These precautions may not result in full control of student access to content and information. As a result, the Public Schools Branch, the Department of Education, Early Learning and Culture, schools, and supervising teachers do not warranty the accuracy, quality, and suitability of the content and information that might be accessed.

**Definitions**

Communication and Information Technology (CIT)

CIT means any device that will store, retrieve, manipulate, transmit or receive digital information. It includes hardware, local and Internet network infrastructure, operating system, networking, and application software.

Digital Citizenship means the norms of responsible behaviour related to the appropriate use of technology.