**2016-2017 TECHNOLOGY ACCEPTABLE USE – From Board Policy #7540.03**

*STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY & GOOGLE APPS USE*

Students are encouraged to use the Board's computers/network and Internet connection for educational purposes. Use of such resources is a privilege, not a right. Students must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action consistent with the Student Handbook, and/or civil or criminal liability. Prior to accessing the Network/Internet at school, students must sign the Student Network and Internet Acceptable Use and Safety Agreement. Parent permission is required for minors.

In addition to network access for district computers, students will also be issued a Google Apps for Education account in our @westottawa.net domain.

***What are Google Apps for Education?***

West Ottawa Public Schools provides staff and students with a Google Apps for Education account. Google Apps is a free web based suite of programs provided by Google for schools to use. Staff and students in West Ottawa Public Schools have access to Google Apps for Education. Google Apps includes such tools as Google Drive, Google Calendar, and Gmail.

All of the Google Apps services can be accessed from anywhere you have an internet connection (school, home, mobile phone, etc.) This reduces and replaces the need for flash drives and/or external data drives. Since Google Apps is all online, it is the same everywhere you use it. There is no issue with having one version of a program at home and a different version at school. Google Apps allows you to easily share documents and files with teachers and other students, so you can turn in assignments electronically and collaborate on projects with classmates.

If you'd like to know more information about the security of data in Google Apps for Education, please visit http://www.google.com/edu/trust.

***WO Student Google Account Setup***

West Ottawa Public School student accounts are created using student cohort year, initials, and a numeric identifier for duplicates, such as 15jrb01. This is the same as their network username.

***Gmail***

Gmail is the powerful Email program that comes with Google Apps for Education. With Gmail you can easily communicate with staff and students within the West Ottawa Public Schools domain.

***Google Calendar***

Google Calendar allows you to maintain multiple calendars for all your needs. You can keep calendars private, or you can share them with others as you determine. You can also invite people to specific events on your calendar.

***Google Drive***

Google Drive gives all users cloud storage space for most file formats. Google Drive can be accessed from any computer with an internet connection. Google Drive allows users to access and share files from any device that has internet connectivity.

**Google Drive includes the following programs:**

Google Documents - word processor similar to Microsoft Word
Google Slides- multimedia presentation tool similar to Microsoft PowerPoint
Google Sheets - spreadsheet program similar to Microsoft Excel
Google Forms - survey/data collection tool for creating forms and collecting data from an audience
Google Drawings - simple graphic design program

***Uses for Student Gmail***

Email can be a powerful communication tool for students to increase communication and collaboration. Students are encouraged to check their email at least once per day. Teachers may send email to middle and high school students to communicate reminders, course content, pose questions related to class work, and such. Students may send email to their teachers with questions or comments regarding class. Students may send email to other students to collaborate on group projects and assist with school classes.

***Student Gmail Permissions***

West Ottawa Public Schools' Gmail system controls who email messages can be sent to and who they can be received from. Gmail is not enabled for students in grades preK-3. Students in grades 4-12 may send and receive email to parent accounts or anyone outside of the district domain. However, the use of student email is subject to monitoring and student have no expectation of privacy within those emails.

***Student Emails to Sta***
Students are encouraged to email staff concerning school-related content and questions. However, there will be no requirement or expectation for staff to answer student email outside of their regular work day, although they certainly may if they choose. For example, an unanswered email to a teacher would not excuse a student from turning in an assignment.

***General Email and Online Chat Guidelines***
Below is a general summary of guidelines related to email and any form of online chat or instant messages: Email and online chat is to be used for school-related communication.

- Do not send harassing email or instant messages or content. Do not send offensive email or instant messages or content. Do not send spam email or instant messages or content.
- Do not send email or instant messages containing a virus or other malicious content.
- Do not send or read email or instant messages at inappropriate times, such as during class instruction. Do not send email or instant messages to share test answers or promote cheating in any way.
- Do not use the account of another person.

Smooth operation of the Board's Network relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

A. Students are responsible for their behavior and communication on the Network/Internet. All use of the Network/Internet must be consistent with the educational mission and goals of the District.

B. Students may only access the Network/Internet by using their assigned Network/Internet/Gmail account. Use of another person's account/address/password is prohibited. Students may not allow other users to utilize their passwords. Students are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/devices when leaving them unattended.

C. Students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the Network/Internet. Students may not intentionally disable any security features of the Network/Internet.

D. Student may not use the Internet to engage in "hacking" or other unlawful activities.

1. Students shall not use the Network/Internet to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a wireless communication device or other electronic equipment is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.

2. Use of the Network/Internet to engage in cyberbullying is prohibited. ""Cyberbullying" is defined as the use of information and communication technologies (such as e-mail, cell phone & text messages, instant messaging (IM), defamatory personal websites and/or blogs, and defamatory online personal polling websites); to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Bill Belsey (http://www.cyberbullying.ca)]

   Cyberbullying includes, but is not limited to the following:

   a. posting slurs or rumors or other disparaging remarks about a student on a website or on weblog;

   b. sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;

   c. using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings or students;

   d. posting misleading or fake photographs of students on websites.

E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

F. Any use of the Network/Internet for commercial purposes, advertising, or political lobbying is prohibited.

G. Students are expected to abide by the following generally-accepted rules of Network/Internet etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Board's computer/Network and Internet. Do not use obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.

2. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet.

3. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.

4. Never agree to get together with someone you "meet" online without prior parent approval.

5. Check e-mail frequently and delete e-mail promptly from the personal mail directory to avoid excessive use of the electronic mail disk space.

6. Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). Students should not delete such messages until instructed to do so by a staff member.

H. Use of Network/Internet to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes or represents in a patently offensive way with respect to what is suitable for minors an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the Board's computers/Network (e.g., viruses) are also prohibited.

I. Malicious use of the Network/Internet to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computing system is prohibited. Students may not engage in vandalism or use the Network/Internet in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass Network/Internet security and/or the Board's technology protection measures. Students must also avoid intentionally wasting limited resources. Students must immediately notify the teacher, building principal, or the Director of Technology if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access (hacking).

J. All communications and information accessible via the Network/Internet should be assumed to be private property (i.e. copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.

K. Downloading of information onto the Board's hard drives is prohibited; all downloads must be to an external storage device such as a USB drive, a student's Google Drive, or a student Chromebook. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or software program that infects the Network with a virus and causes damage, the student will be liable for any and all repair costs to make the Network once again fully operational.

L. Students are prohibited from accessing or participating in online "chat rooms" or other forms of direct electronic communication (other than e-mail) without prior approval from a teacher. All such authorized communications must comply with these guidelines.

M. Privacy in communication over the Internet and the Network is not guaranteed. To ensure compliance with these guidelines, the Board reserves the right to monitor, review, and inspect any directories, files and/or messages residing on or sent using the Board's computers/Network. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

Users have no right or expectation to privacy when using the Network/Internet. The District reserves the right to access and

inspect any facet of the Network/Internet, including, but not limited to, computers, devices, Network or Internet connections, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein.

A student's use of the Network/Internet constitutes his/her waiver of any right to privacy in anything he or she creates, stores, sends, transmits, uploads, downloads or receives on or through the Network/Internet and related storage medium and equipment.

Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to discovery that a user has violated Board policy and/or law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials. Students' parents have the right to request to see the contents of their children's files, e-mails and records.

N. Use of the Network/Internet and any information procured from the Network/Internet is at the student's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions. The Board is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Network/Internet sources used in student papers, reports, and projects should be cited the same as references to printed materials.

O. Disclosure, use and/or dissemination of personal identification information of minors via the Network/Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Network and Internet Acceptable Use and Safety Agreement Form."

P. Proprietary rights in the design of web sites hosted on the Board's servers remains at all times with the Board.

Any individual who is aware of a violation of the Board policy or this guideline, including inappropriate on-line contact, content, or conduct, such as sexting, harassment or cyberbullying, should bring it to the attention of the school principal or Superintendent immediately.

# 2016-2017 TECHNOLOGY ACCEPTABLE USE ACKNOWLEDGEMENT FORM

Parent/Guardian and/or Student:

1. **Please remove the top pages and keep for your records.**
2. **Please complete and sign the Confirmation below; and return it per the following instructions:**

***Kindergarten-5th Grade Students:*** Return this Confirmation page to your teacher.

***6th – 12th Grade Students:*** Return this Confirmation page to your school office.

**West Ottawa Public Schools Acceptable Use Policy Confirmation**

I have read and understand the Acceptable Use Policy of West Ottawa Public Schools. I agree to adhere to the policy and understand there will be consequences if I do not.

_____ _____

Student Name (Please print) Student Signature

_____ _____

Building/School Date

I have read and understand the Acceptable Use Policy of West Ottawa Public Schools. I also understand that my son or daughter must adhere to this policy, and that there will be consequences if he/she does not. Additionally, I understand the n uses and limitations of filter technology in accessing information on the Network/Internet.

_____ _____

Parent/Guardian Name (Please print) Parent/Guardian Signature