Breitung Township Schools Internet Safety Policy
Network Acceptable Use Policy (AUP), and
Bring Your Own Device Policy (BYOD)

The Breitung Townships Schools Internet Safety Policy applies to all students and covers all use of technology resources including computer hardware, software, and network resources. It includes the Acceptable Use Policy (AUP) for using technology as well as policies regarding Bringing Your Own Device (BYOD) to connect to the network and Internet. The use of the Internet is a privilege, not a right, and inappropriate use may result in termination of those privileges for a student.

This Internet Safety Policy is in addition to the District's Bylaws and Policies (a.k.a. NEOLA Policies). A copy of the District "Bylaws and Policies" can be found on our website at www.kingsford.org.

The Technology resources that are provided by the Breitung Township School District are available to enhance teaching and learning, facilitate professional development, and support school business systems.

Internet Safety Policy: It is the policy of The Breitung Township Schools to:

(a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
(b) prevent unauthorized access and other unlawful online activity;
(c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors (FERPA); and
(d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions:

- AUP: Acceptable Use Policy and refers to the acceptable use of the school network, technology resources, and Internet connection.
- BYOD: Bring Your Own Device and refers to student-owned Internet-enabled wireless devices. These devices include any internet enabled device such as laptops, netbooks, MAC Books, iPods, iPads, Kindles, Droids, Blackberries, smart phones, etc.
- CIPA: Children's Internet Protection Act
- MINOR. The term "minor" means any individual who has not attained the age of 17 years.
- Other definitions are defined by CIPA

Access to Inappropriate Material: To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, (e-mail, chat rooms, instant messaging) to inappropriate information. Specifically, as required by CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be modified for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

BYOD: Beginning in the 2012-2013 school year, Breitung Township Schools may allow students to bring their own wireless devices provided they adhere to and sign off on the Internet Safety Policies of the District. The purpose of BYOD is to allow students to access school network resources, including the Internet, from their mobile devices. Such access is intended to enhance learning and will allow students

greater opportunity for developing 21st Century skills: critical thinking and problem solving; communication; collaboration; and creativity and innovation. As teachers incorporate more 21st Century teaching in their classrooms, students will be able to access the classroom content and learn anytime, anywhere.

How to Access the Internet from Wireless Device? – The Network ID and passcode will be provided to all students of BTS. Students are required to use only the BTS Internet connection from any student owned device while on the premises at BTS.

Cellular Data Network – Using a Cellular Data network while on school premises is a violation of this policy and is subject to disciplinary action. This is because the BTS Internet is filtered and monitored, and Cellular Data Networks are not. If a student is suspected of using his/her device to access the Cellular Data Network, school authorities may search the device for evidence of Cellular Data Network use.

Acceptable uses for student owned device – Accessing the Internet for research in educational areas, communicating through school-provided E-Mail account, collaborating on a teacher-approved Web 2.0[1] Internet Sites. Web 2.0 sites allow student to become active participants in Creating, Collaborating, and Communication in an educational setting.

Examples of Inappropriate Network Uses (including BYOD) – Technology Resources, the Network the Internet and student-owned devices may not be used for:

- Disruption
- Cheating
- Violation of person's privacy
- Actions compromising personal and/or school safety
- Cyber Bullying – Posting malicious remarks electronically on the Web or by E-Mail.
- Other illegal and/or unethical activities
- Transmitting obscene, abusive or inappropriate language or images
- Violation of the law
- Altering system software
- Placing unauthorized information, computer viruses or harmful programs on computers
- Sharing personal passwords or using someone else's password
- Unauthorized access including so-called 'hacking'
- Unauthorized access to E-Mail other than the school issued E-mail account
- Unauthorized disclosure, use and dissemination of personal identification information regarding minors
- Any other conduct that violates another discipline code as outlined in the school's student handbook

[1] Web 2.0 Sites allows users to contribute, collaborate and create content and save their work so that it can be accessed anytime, anywhere. Web 2.0 includes features such as blogging, social bookmarking, social networking, podcasting, and RSS Sharing.

Portable electronic devices (BYOD or school owned devices), are prohibited from being used in the following locations:

- Restrooms
- Locker rooms
- Classrooms where the teacher does not give explicit permission to use the device (It is up to individual teachers to develop their own policies regarding the use of the student-owned devices in their classrooms. The teacher's policies will be communicated to the students in their "classroom rules".)

Internet Safety Education: Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security.

Internet and Network Usage Monitoring: Online activities may be monitored by instructors or administrators at any time. Monitoring may include, but is not limited to, visual observation during class sessions or use of specific monitoring tools and software to review browser history and network, server and computer logs.

Transferring Files from Home to School: When students needs to transfer electronic files between their home computer and their school computer, they can do so in a variety of ways. The preferred methods are to upload the file to their school issued e-mail box or to e-mail the file to their teacher. Students may also copy the file to removable storage media and bring it to school and copy the file from the removable media to the student's home directory. Executable files (.exe), zip files (.zip), and batch files (.bat) are not permitted.

Removable Media: Students may use certain types of removable media to transfer files between school and home only with permission from their teacher or media specialist and must follow the rules outlined here:

1. Inspect the disk or USB drive for mechanical imperfections. Don't insert devices that look damaged into a District-owned computer.
2. Insert the disk or drive into the teacher computer. Do not force anything. If it doesn't fit in smoothly, it may be damaged.
3. Allow your computer to detect new hardware (if it is a USB drive)
4. Open My Computer
5. Right click on the drive and select "Scan for Viruses"
6. If a virus is detected, you may attempt to remove the virus using the antivirus software that is installed on the computer.
7. If no viruses are detected continue with these steps:
    a. Double click on the drive to view the contents of the drive. <u>If the drive contains any .exe, .zip, or .bat files, it may not be used to transfer files.</u>
8. If the teacher or media specialist has access to the student's home directory, then the teacher should copy the file from the removable device into the student's home directory. If the teacher does not have access to the student directory, then they must have the student log onto a computer in the classroom or media center.

9. Observe and assist the student with copying files from the device to their home directory.
10. Upon completion of file transfer, eject the CD or right click on the removable drive icon in the system tray and select "Safely remove hardware."

Warranties: The Breitung Township School District does not warrant computer or network functionality or accuracy of information found on the Internet. In addition, the District does not warrant against lost or corrupted data that may be accessed or stored on District computers or servers or student-owned devices. On occasion, an inappropriate website may get through the Internet filter. Students should bring the website in question to the attention of a staff member who shall contact the District Technology Personnel, so that these websites can be added to the blocked site list.

Photographs of student on the Breitung Township Schools Web Pages: Teachers and students create the web pages that are published on our web site which is located at www.kingsford.org. Occasionally, photographs of students will appear on some of those pages. It is our policy not to include the full name of the student unless a parent/guardian has granted permission to use their child's full name. By signing the attached, you grant the District permission to display your child's photograph with their full name. However, as a general rule, it is our practice not to include the full name of the student at the elementary school.

Ownership of Student-Produced Computer Materials: Rights of ownership to any computer material, instructional material or devices shall be the exclusive property of the District when any such item is produced by a student utilizing district supplies and / or equipment as a dominate resource in producing materials.

Consequences and Disciplinary Action: If a student is suspected of misuse of their device, authorities may confiscate and search the mobile device and take disciplinary action against the student. Disciplinary action may include but is not limited to, having their BYOD privilege suspended or terminated permanently, banned from using the Internet on school-owned devices, banned from using any school owned computers, suspension, and expulsion.

Adoption This Internet Safety Policy was adopted by the Board of Breitung Townships Schools at a public meeting, following normal public notice, on June 25, 2012.

Parent and Student Signature Forms: Students and parents are required to sign a written agreement to abide by the terms and conditions of this policy before students are permitted access to the technology resources of the District. By signing the form, they agree to the terms of on the Internet Safety Policy, AUP and BYOD and policies. Even if the students do not currently own a wireless device, they must sign the document in order to be allowed access to the Internet.

Breitung Township School District
Computer User Agreement and Release Form

Student:_____
(Please print name)
Grade:_____ School Year: _____

In consideration for the privileges of using the District and/or Network resources, including Internet, I agree to abide by the Internet Safety Policy, Acceptable Use Policy and BYOD Policy which include, but are not limited to, the information contained on pages 1 through 4 of this form.

I also have read and agree to abide by the policy for using removable media to transfer files to/from home and school computers. I also understand that misuse of Network resources, the Internet or the removable media policy will result in disciplinary action and the loss of technology privileges at Breitung Township Schools.

_____ _____

Signature of Student Date

As the student's parent or legal guardian, I agree to the terms of this policy and I hereby release the District, Network, their operators and administration from any and all claims, fees, expenses or damages incurred as a result of my child's misuse of the Network resources or Internet.

_____ _____

Signature of Parent Date

I agree to allow photographs of my child to appear on the school's web site in accordance with the District policy outlined on page 4.

_____ _____

Signature of Parent Date

(Please keep page 1-4 for future reference. Sign and return this page to the school office.)